FOUES50 +80T 7950

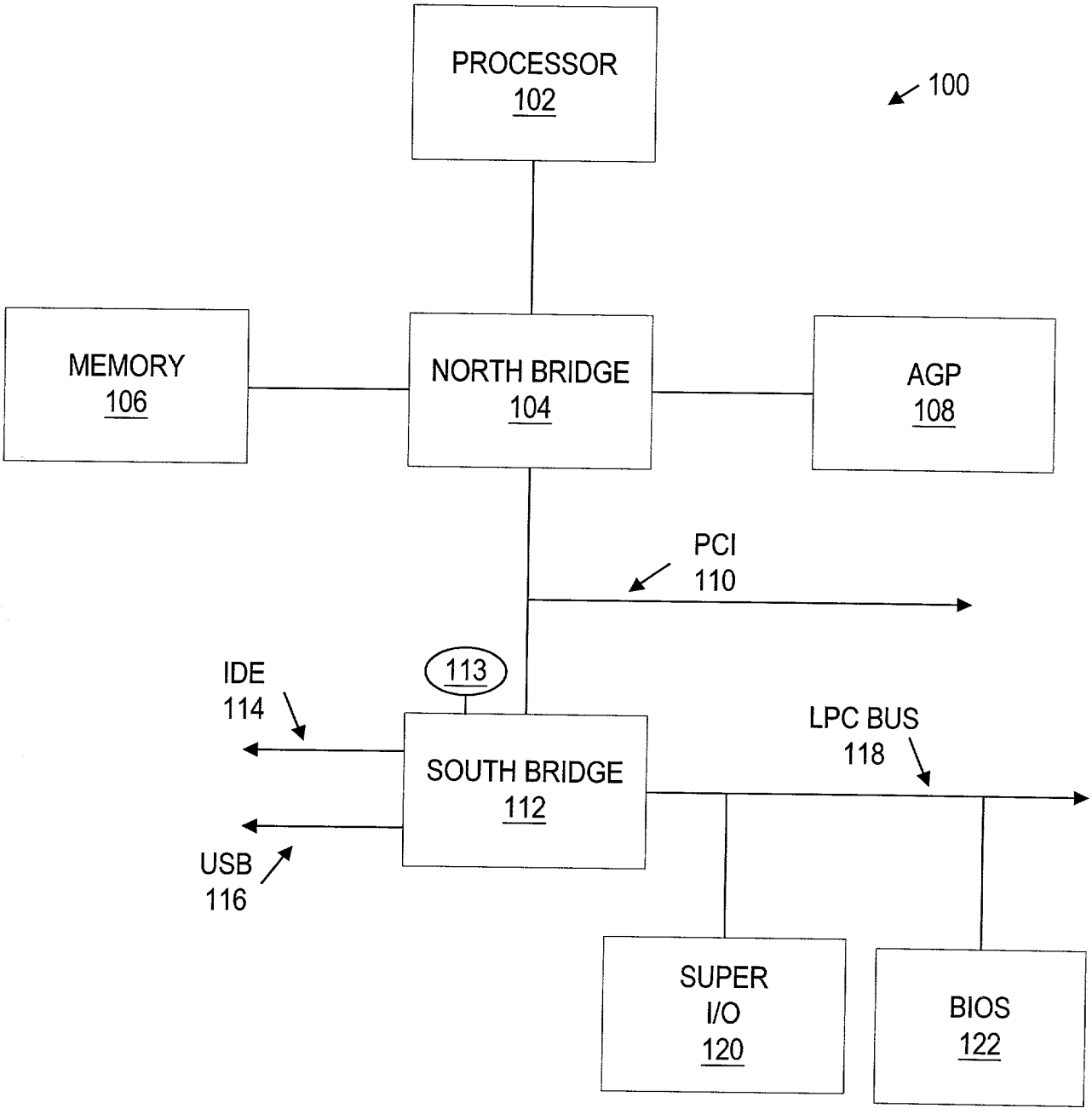


Fig. 1A
(Prior Art)

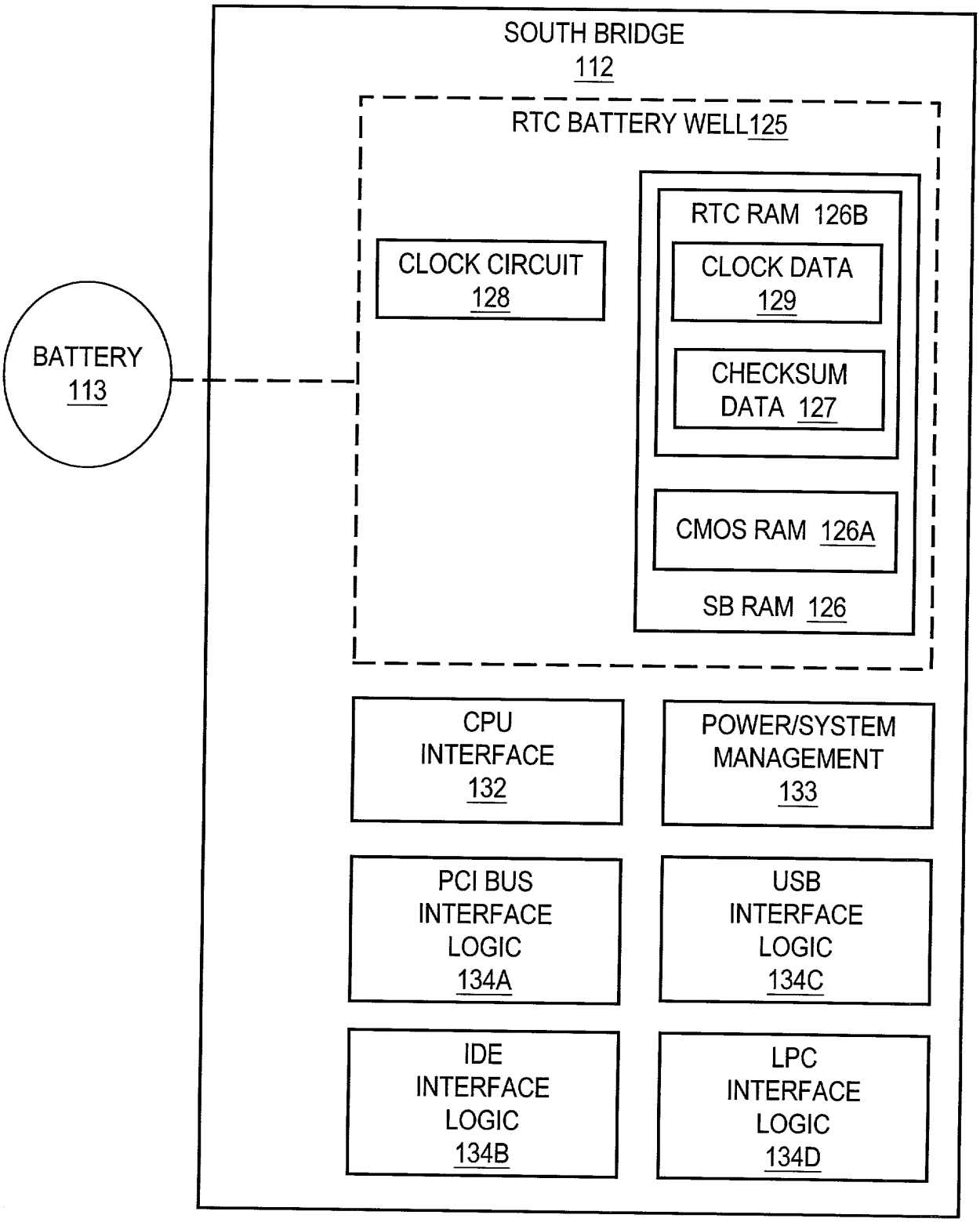


Fig. 1B
(Prior Art)

EXHIBIT 1004, PAGE 0073

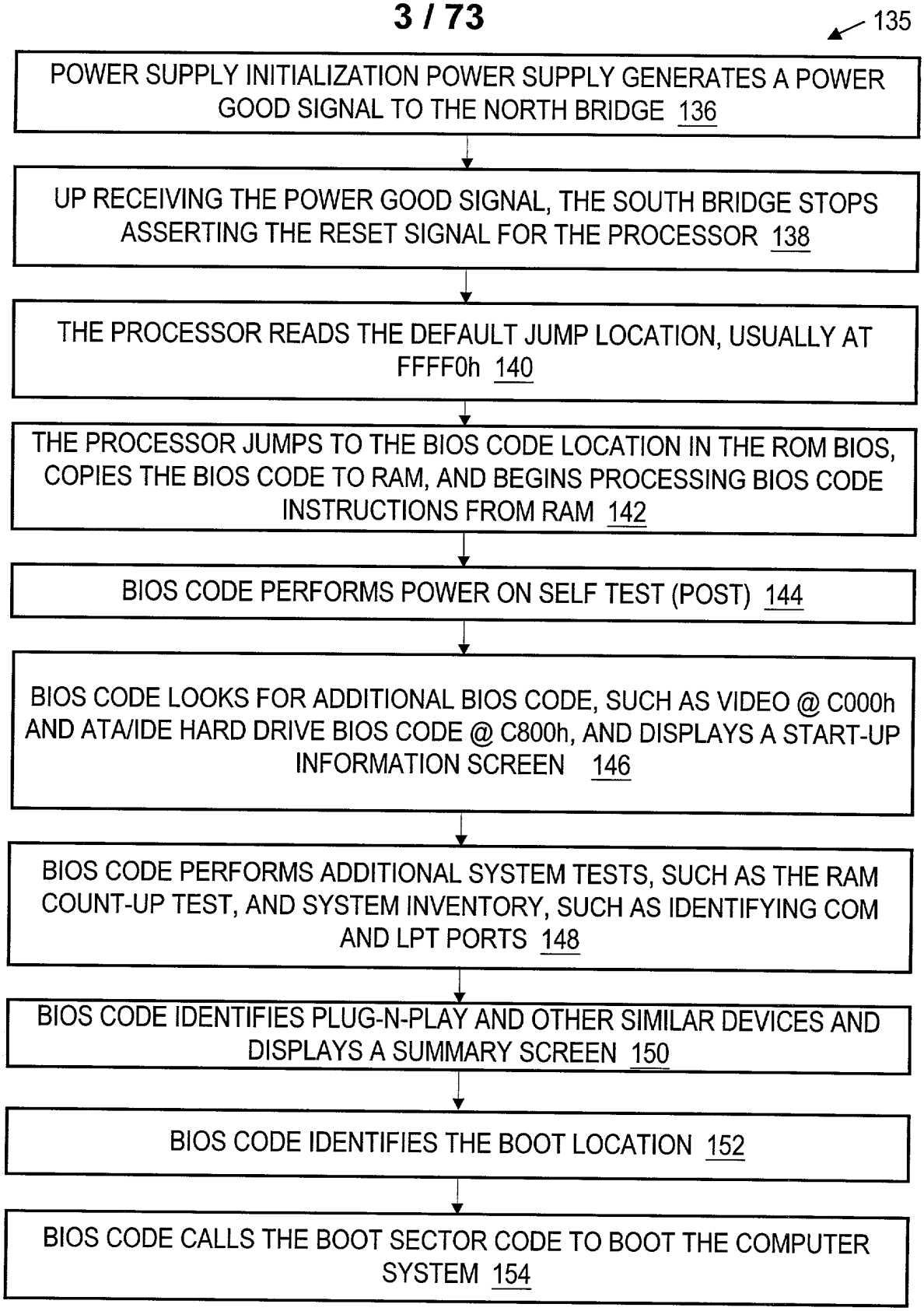


Fig. 2A
(Prior Art)

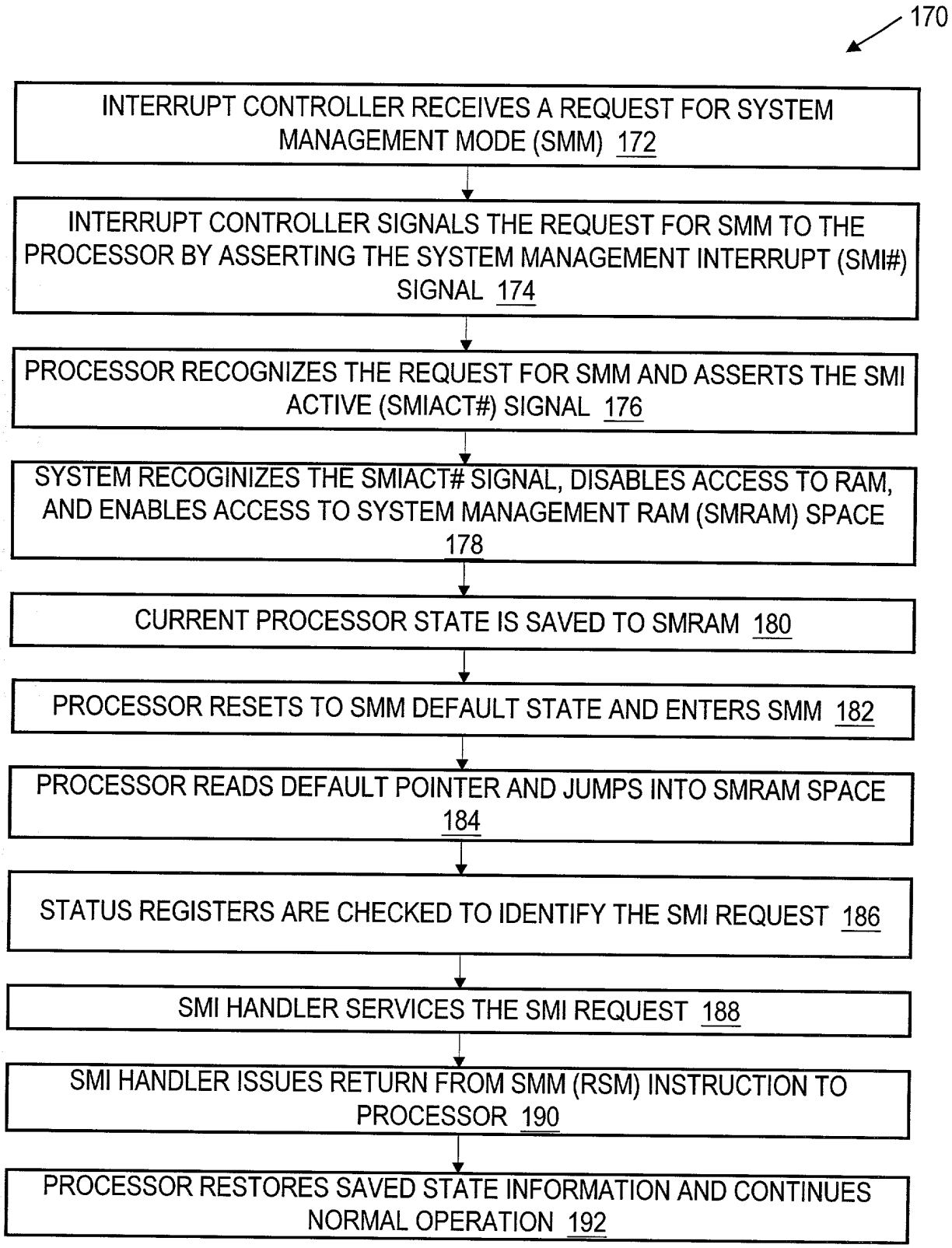


Fig. 2B
(Prior Art)

Processor-Ref-2650

TDD650 "19DT/960

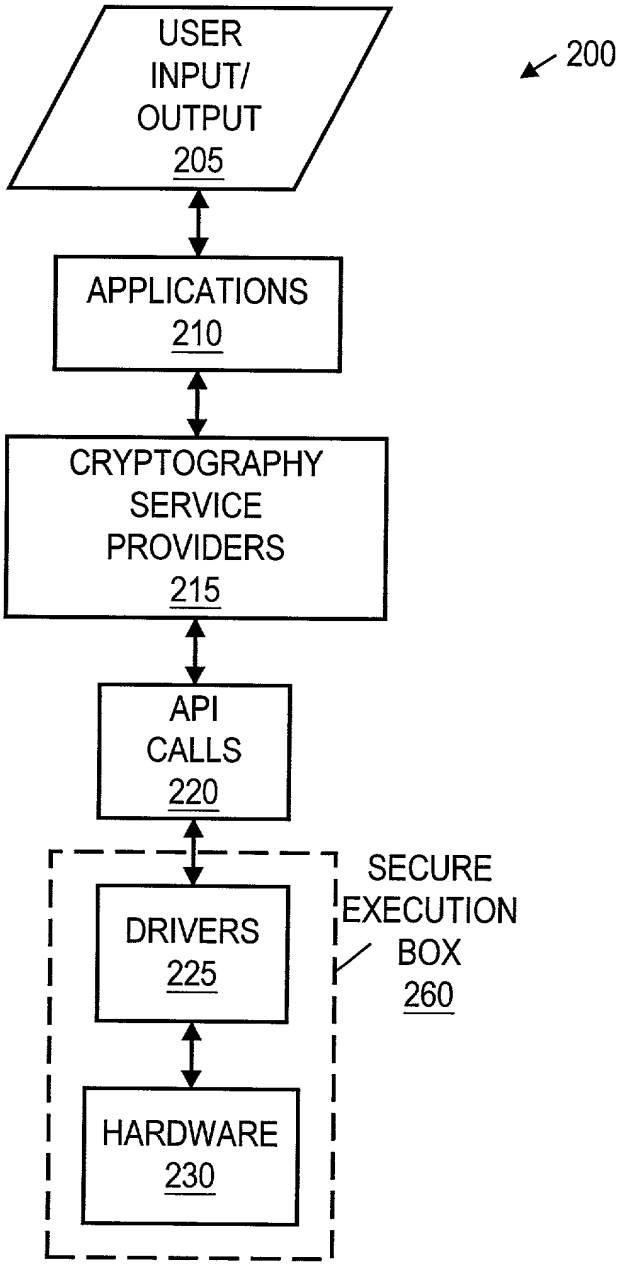


Fig. 3

Petitioner Apple Inc. - Exhibit 1009, p. 6

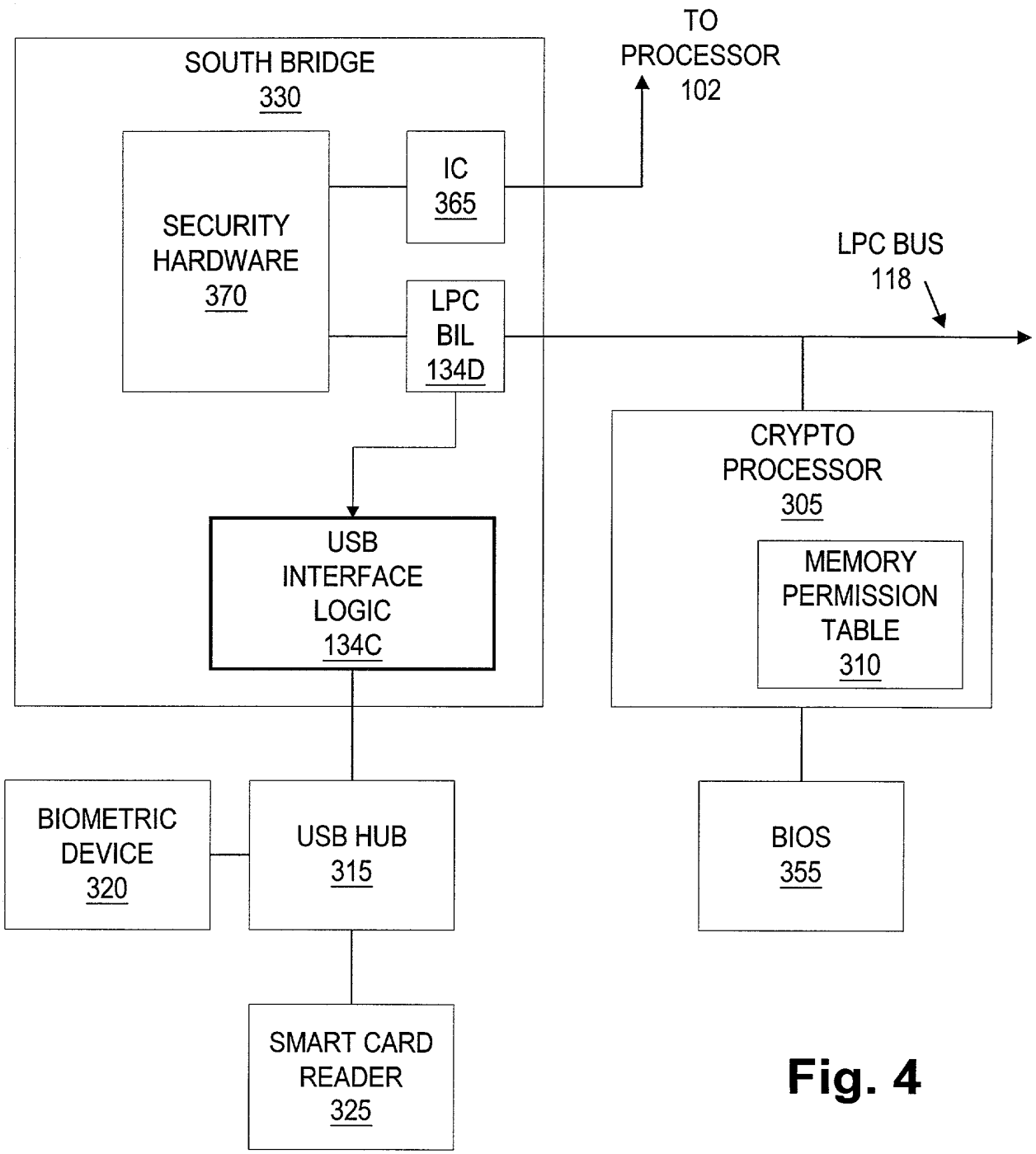


Fig. 4

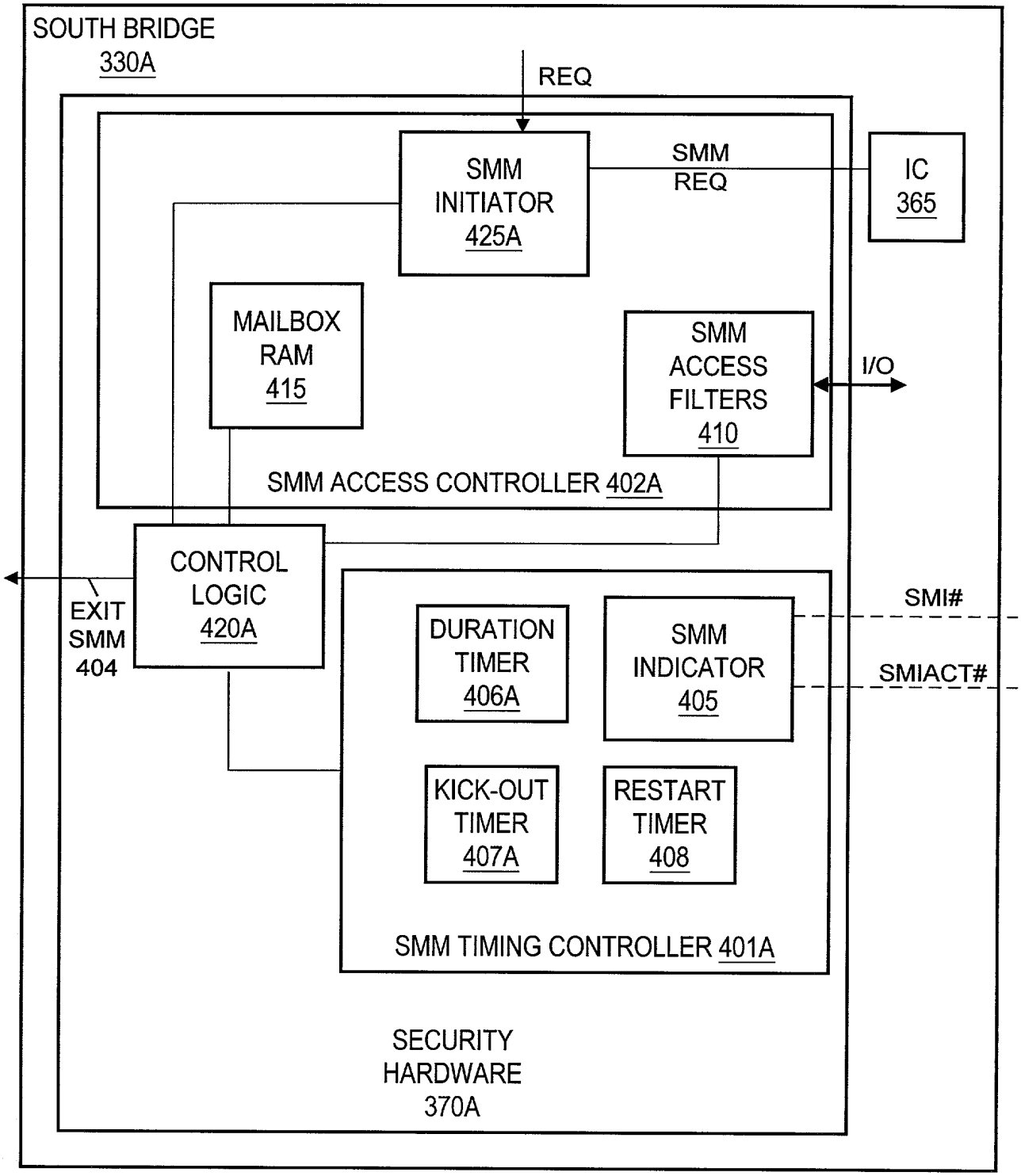

SOUTH BRIDGE
330A
REQ
SMM
INITIATOR
425A
SMM
REQ
IC
365
MAILBOX
RAM
415
SMM
ACCESS
FILTERS
410
I/O
SMM ACCESS CONTROLLER 402A
CONTROL
LOGIC
420A
EXIT
SMM
404
DURATION
TIMER
406A
SMM
INDICATOR
405
SMI#
SMIACT#
KICK-OUT
TIMER
407A
RESTART
TIMER
408
SMM TIMING CONTROLLER 401A
SECURITY
HARDWARE
370A

Fig. 5A

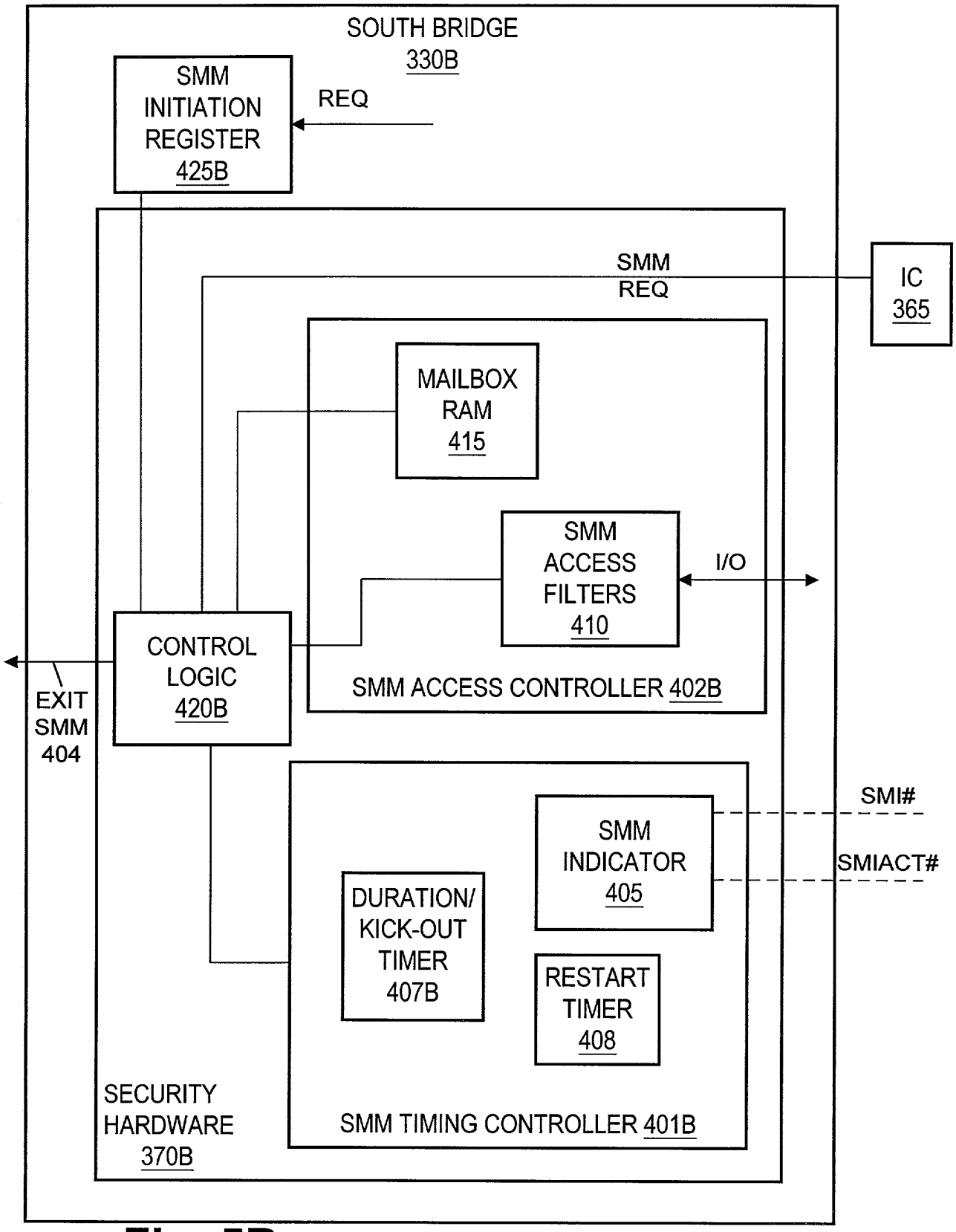


Fig. 5B

FOSS0-1930F7360

1005550-1801-7350

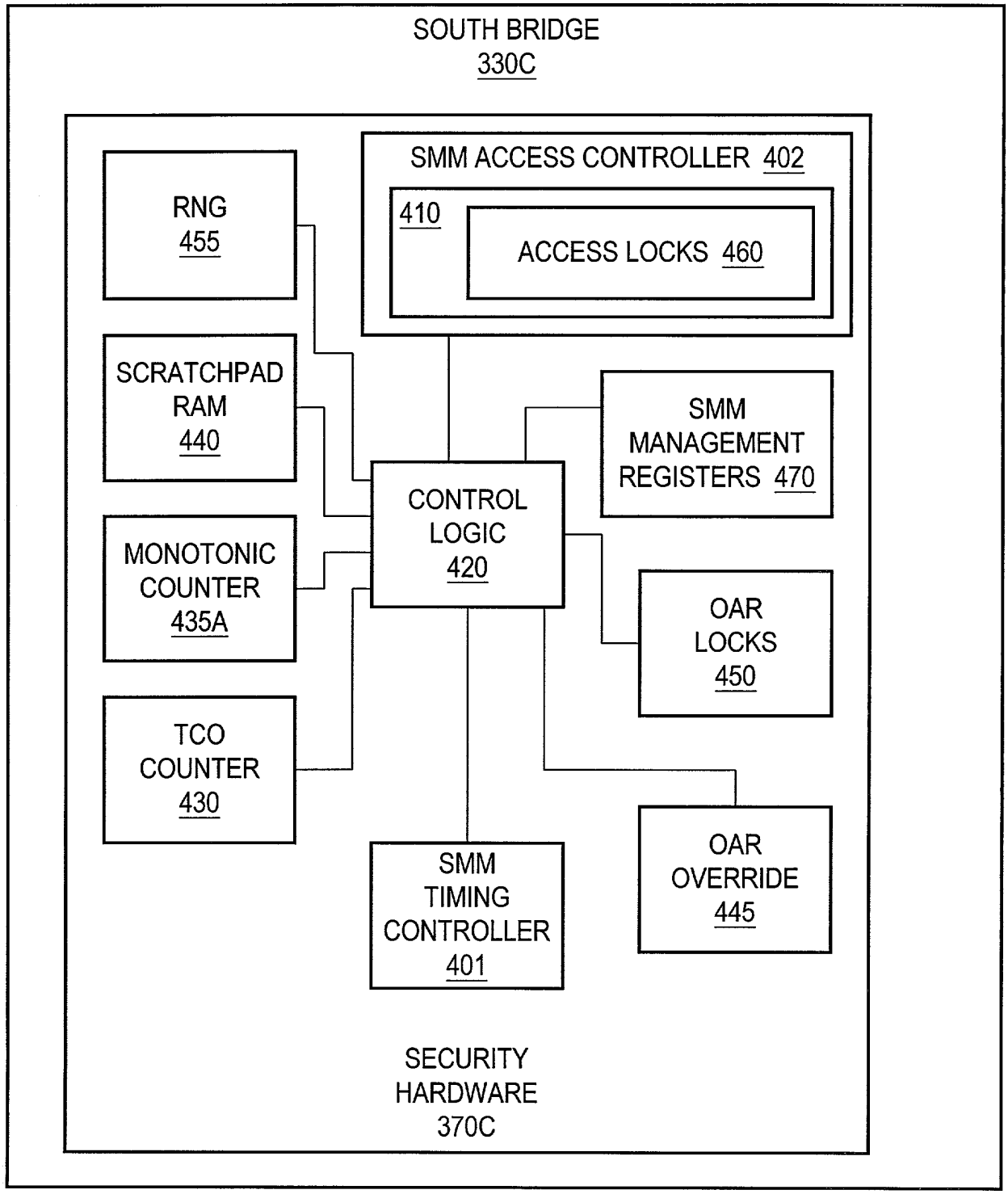


Fig. 6

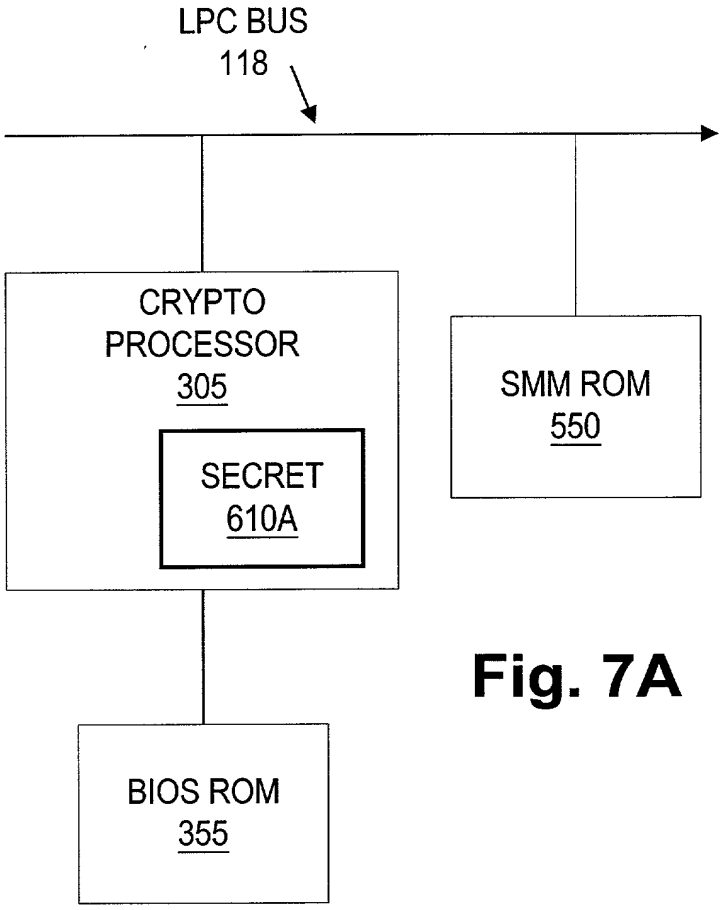


Fig. 7A

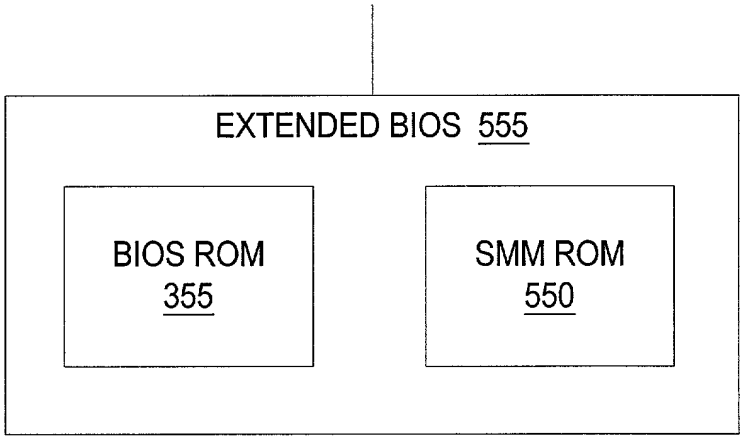


Fig. 7B

TT3763 - 10/73/650

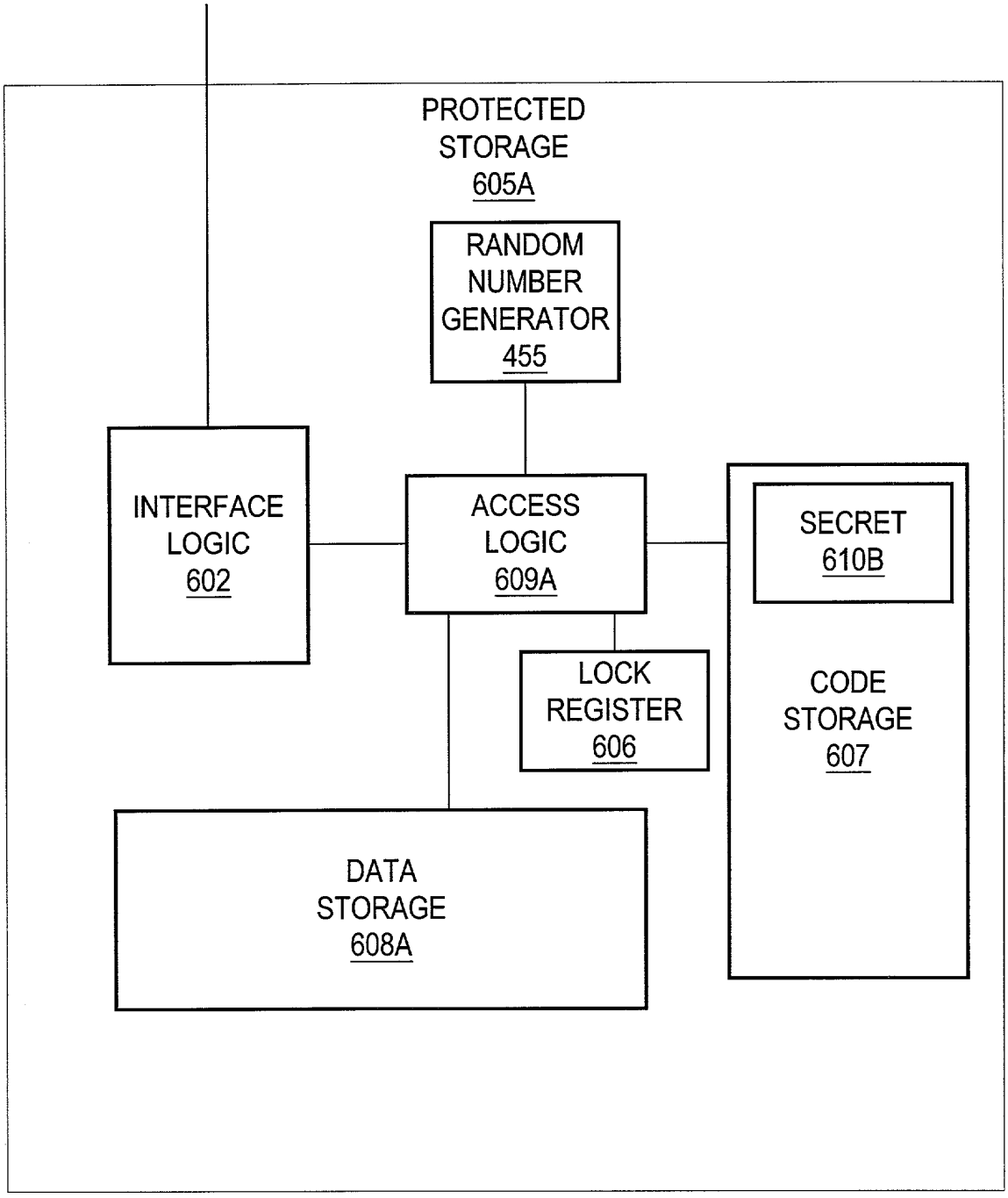


Fig. 7C

T0025.0 +180F7360

7005501 "4801 7360

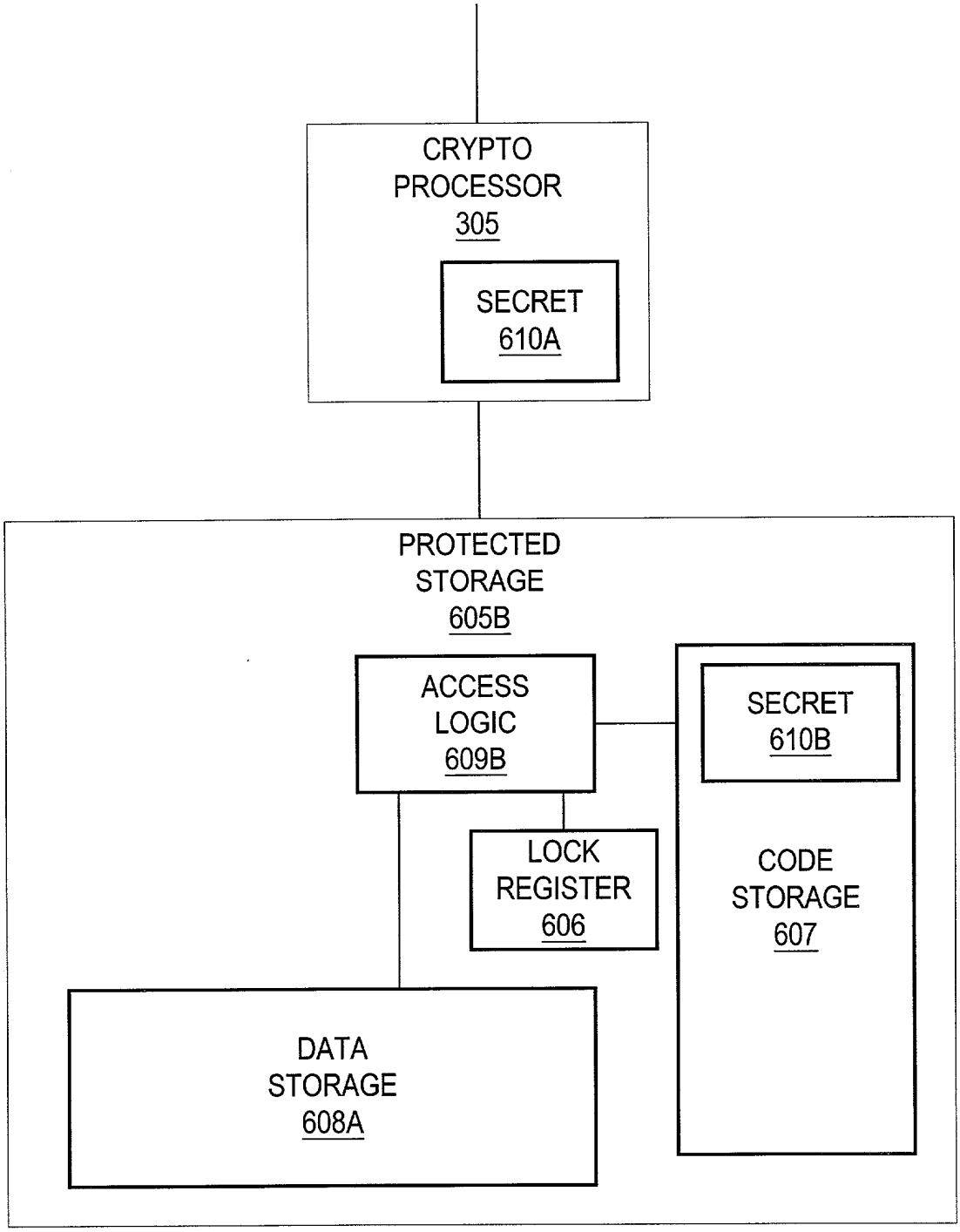


Fig. 7D

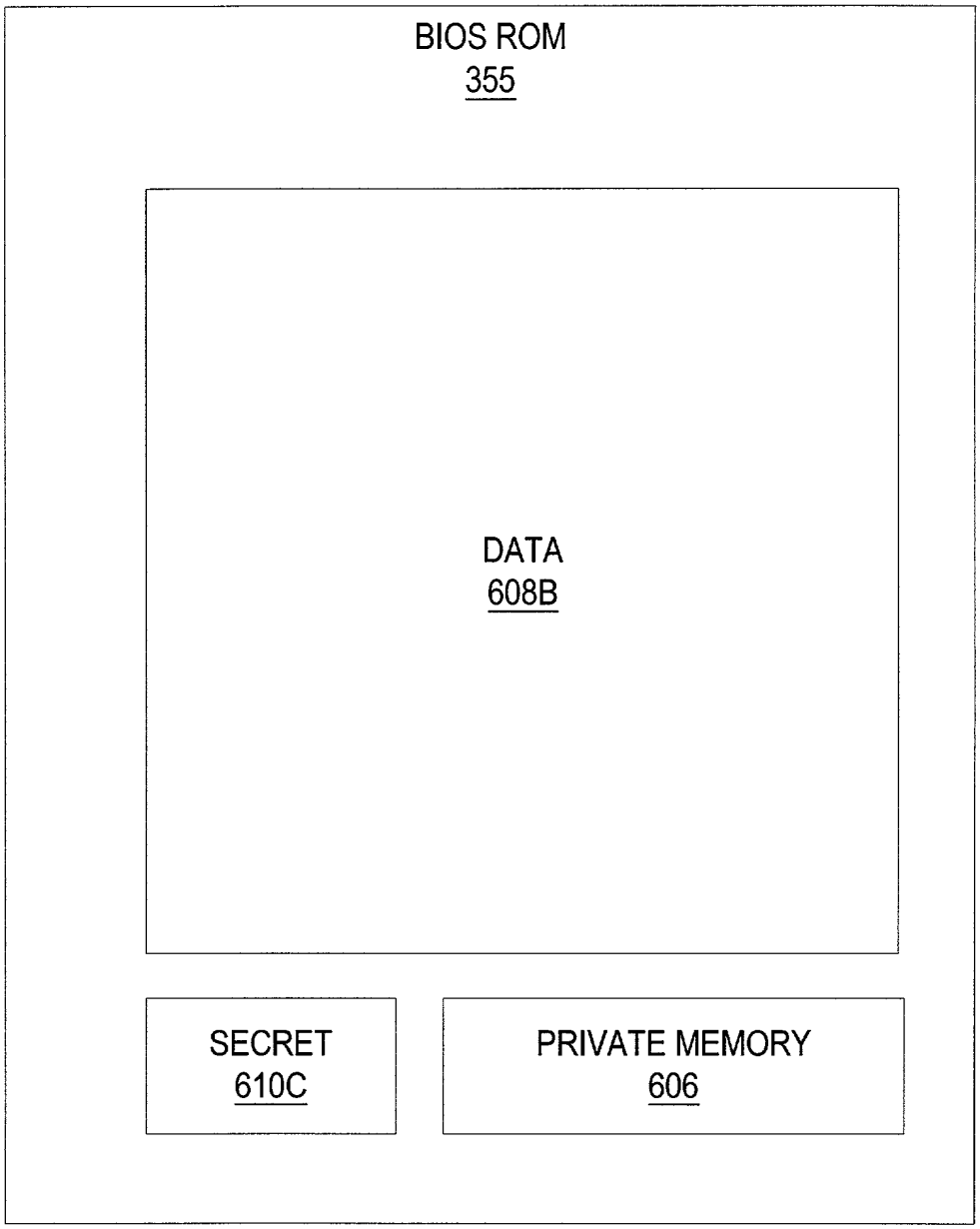


Fig. 8A

Tc0025 0 4 5 0 4 5 0 0 4 5 0

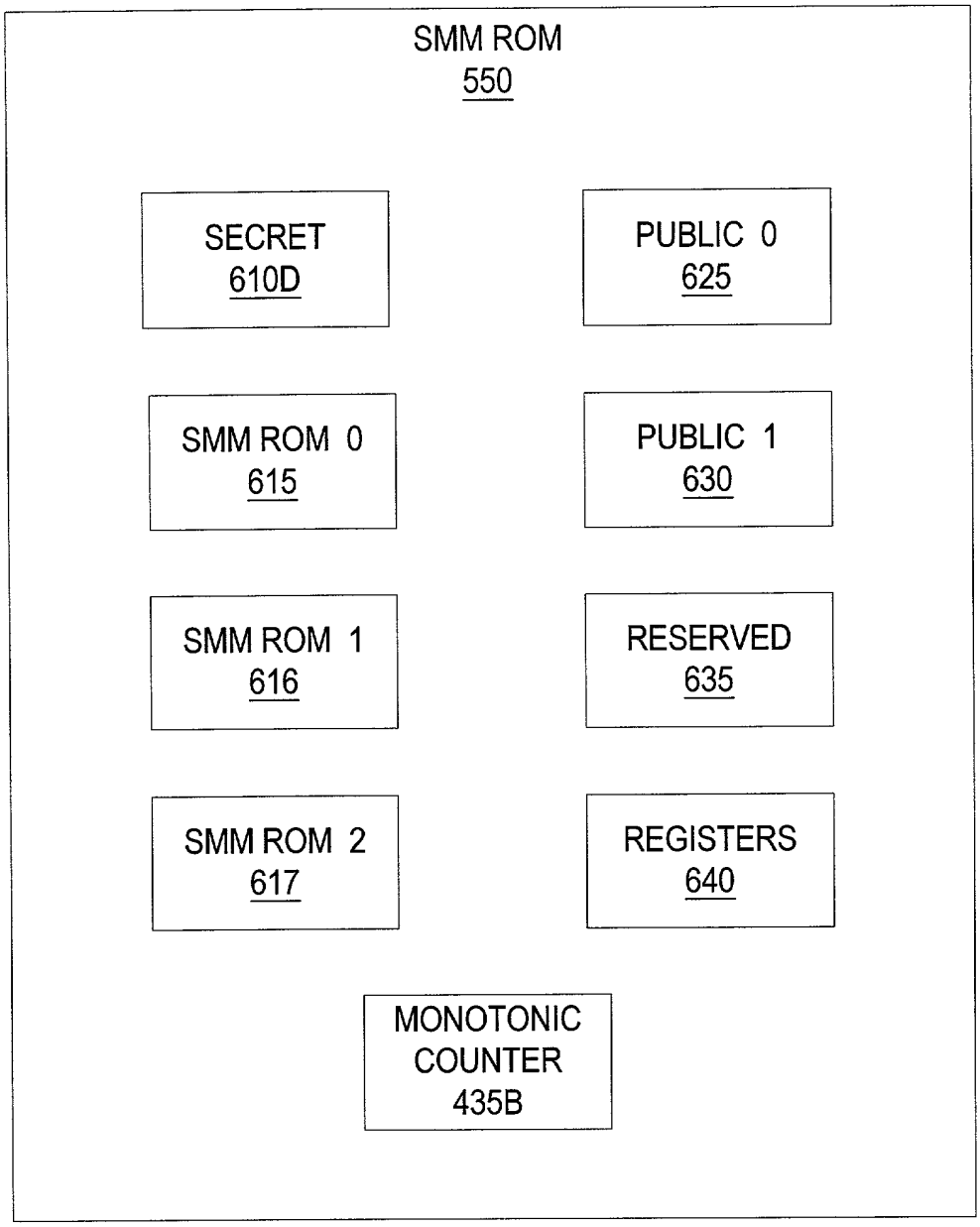


Fig. 8B

FOUNDATION EXHIBIT 2060

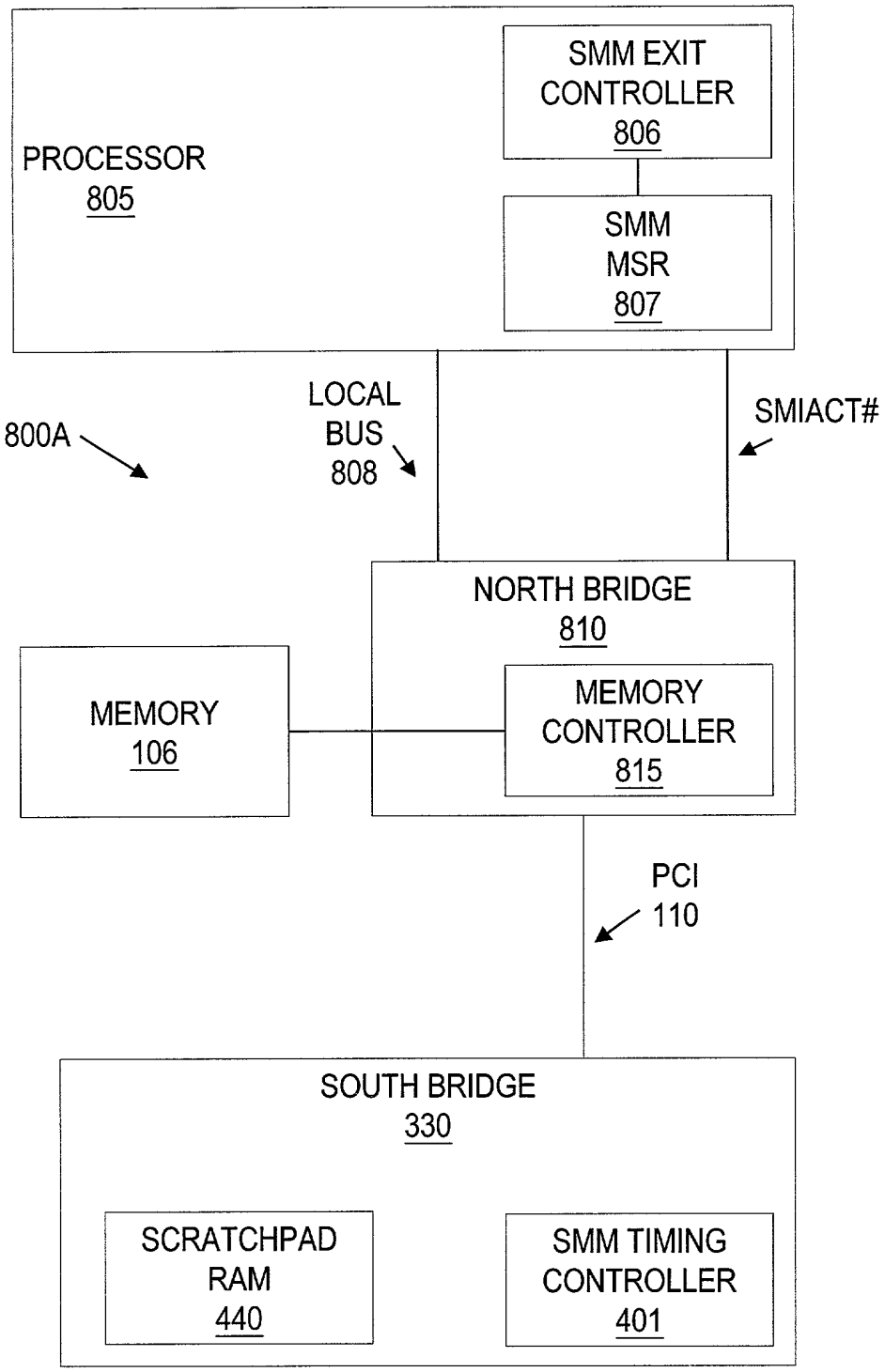


Fig. 9A

FOUR-SIDE-180F/360

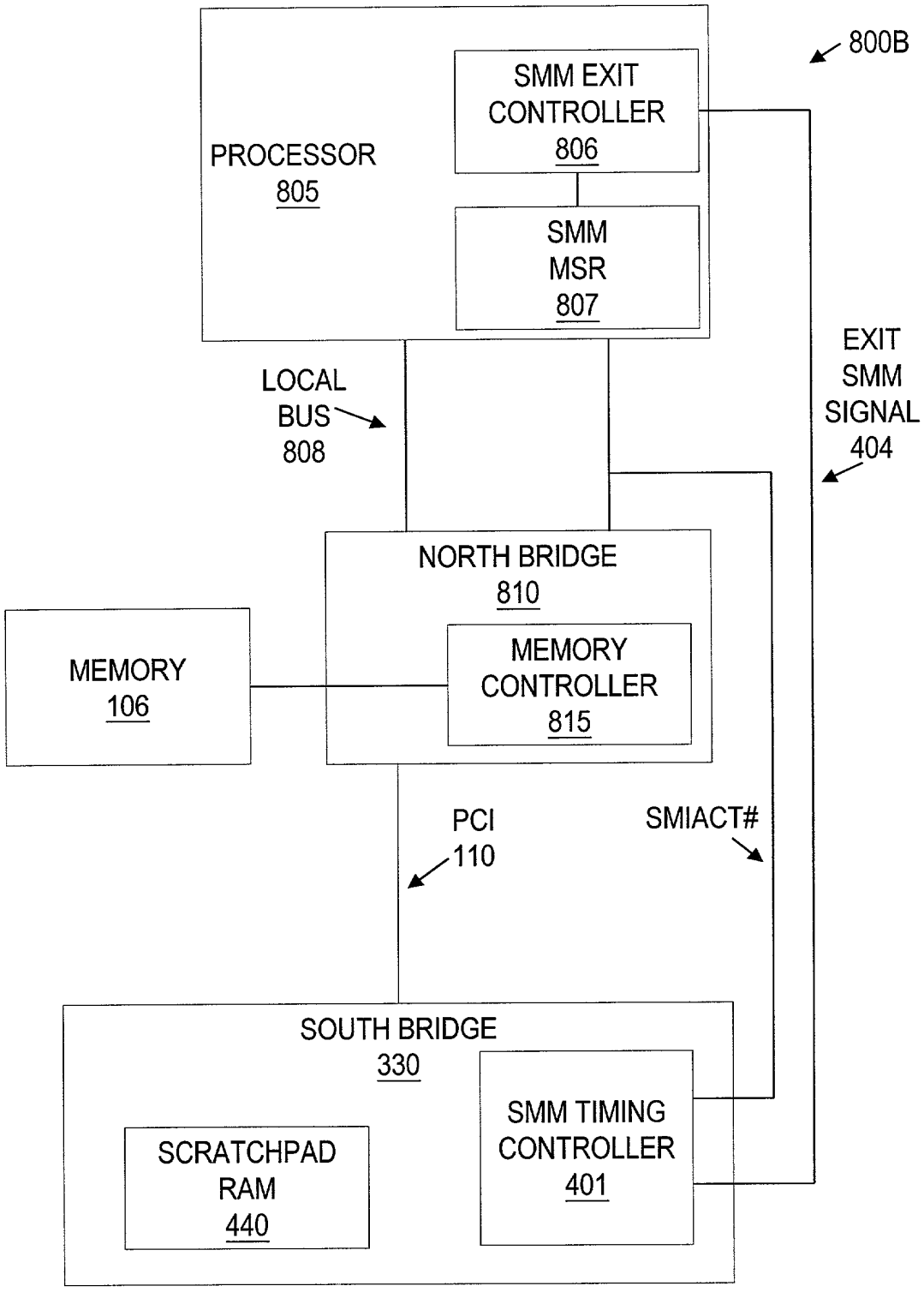


Fig. 9B

FOR SALE - 1800 PAGES

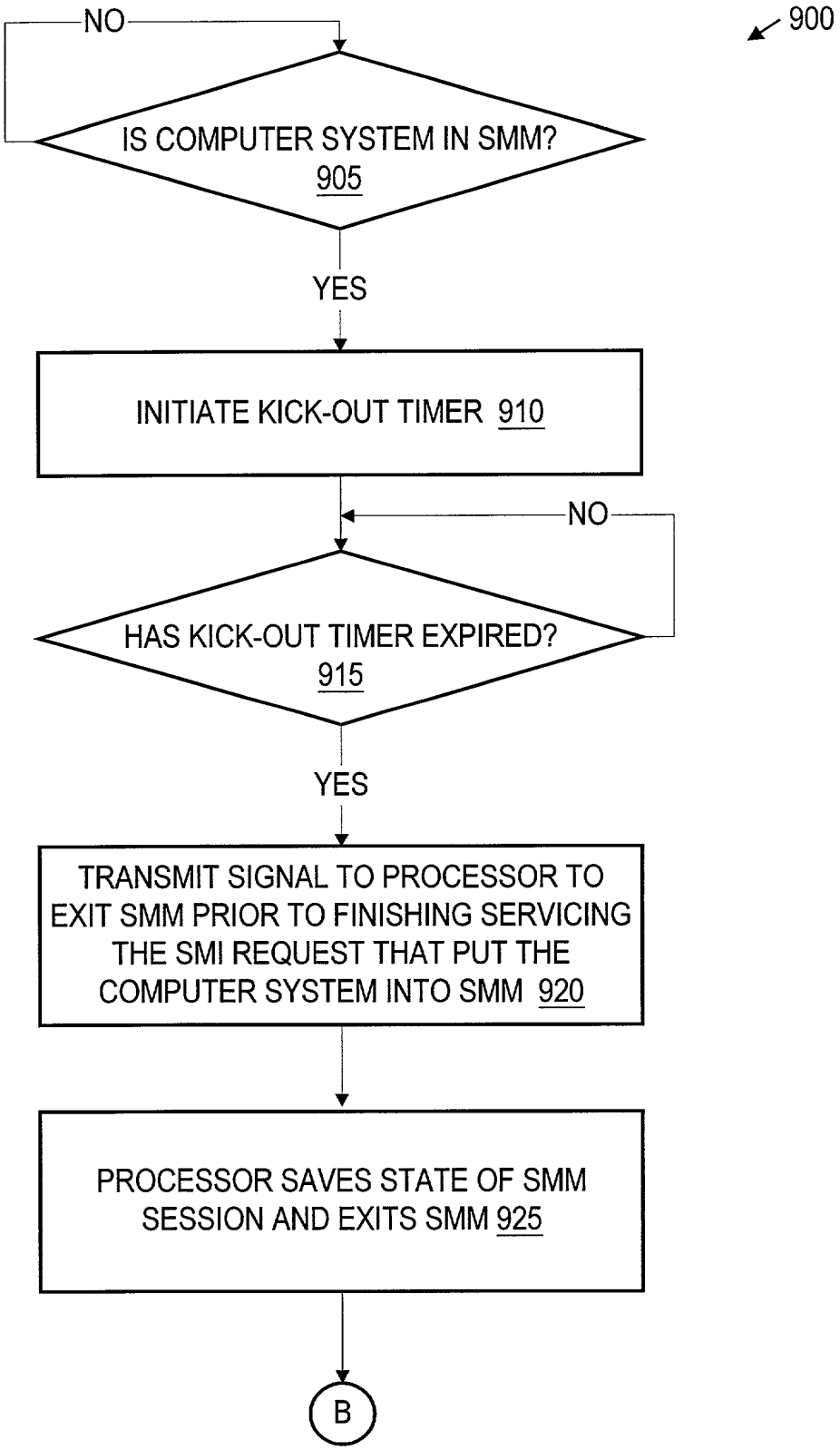

900
NO
IS COMPUTER SYSTEM IN SMM? 905
YES
INITIATE KICK-OUT TIMER 910
NO
HAS KICK-OUT TIMER EXPIRED? 915
YES
TRANSMIT SIGNAL TO PROCESSOR TO EXIT SMM PRIOR TO FINISHING SERVICING THE SMI REQUEST THAT PUT THE COMPUTER SYSTEM INTO SMM 920
PROCESSOR SAVES STATE OF SMM SESSION AND EXITS SMM 925
B

Fig. 10A

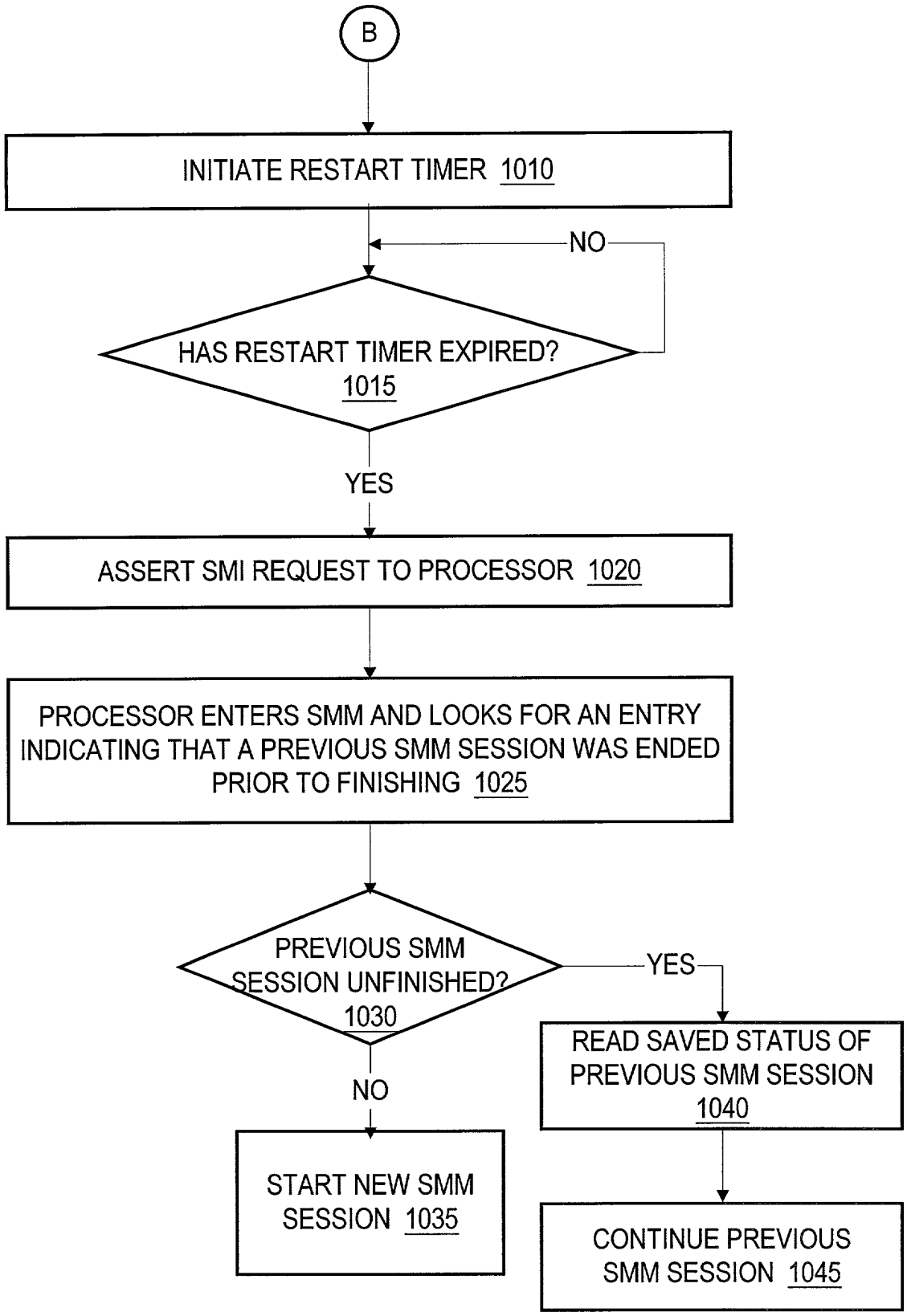


Fig. 10B

0567-0064-0590-1001

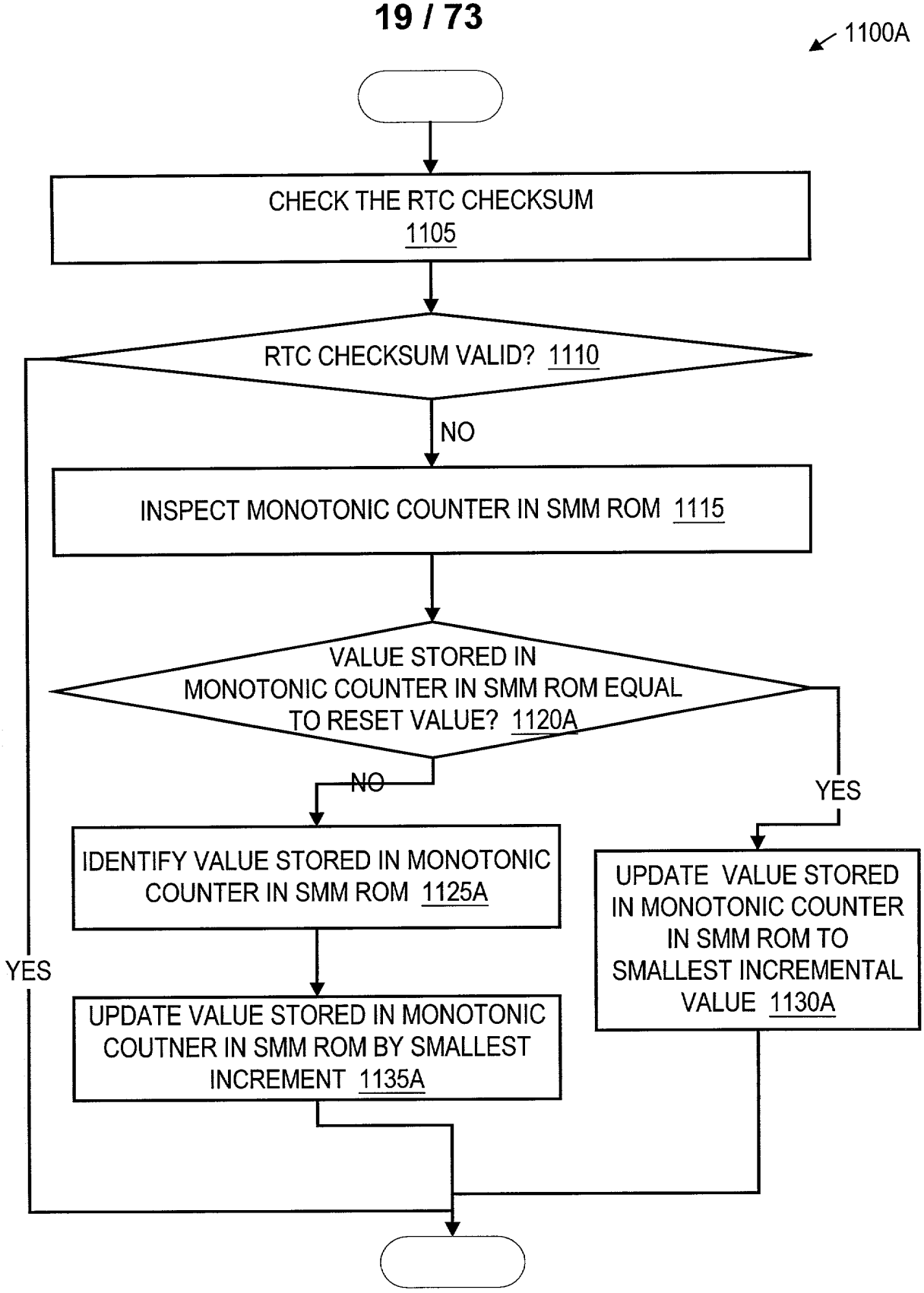

1100A
CHECK THE RTC CHECKSUM 1105
RTC CHECKSUM VALID? 1110
NO
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1115
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE? 1120A
NO
YES
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM 1125A
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT 1135A
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE 1130A

Fig. 11A

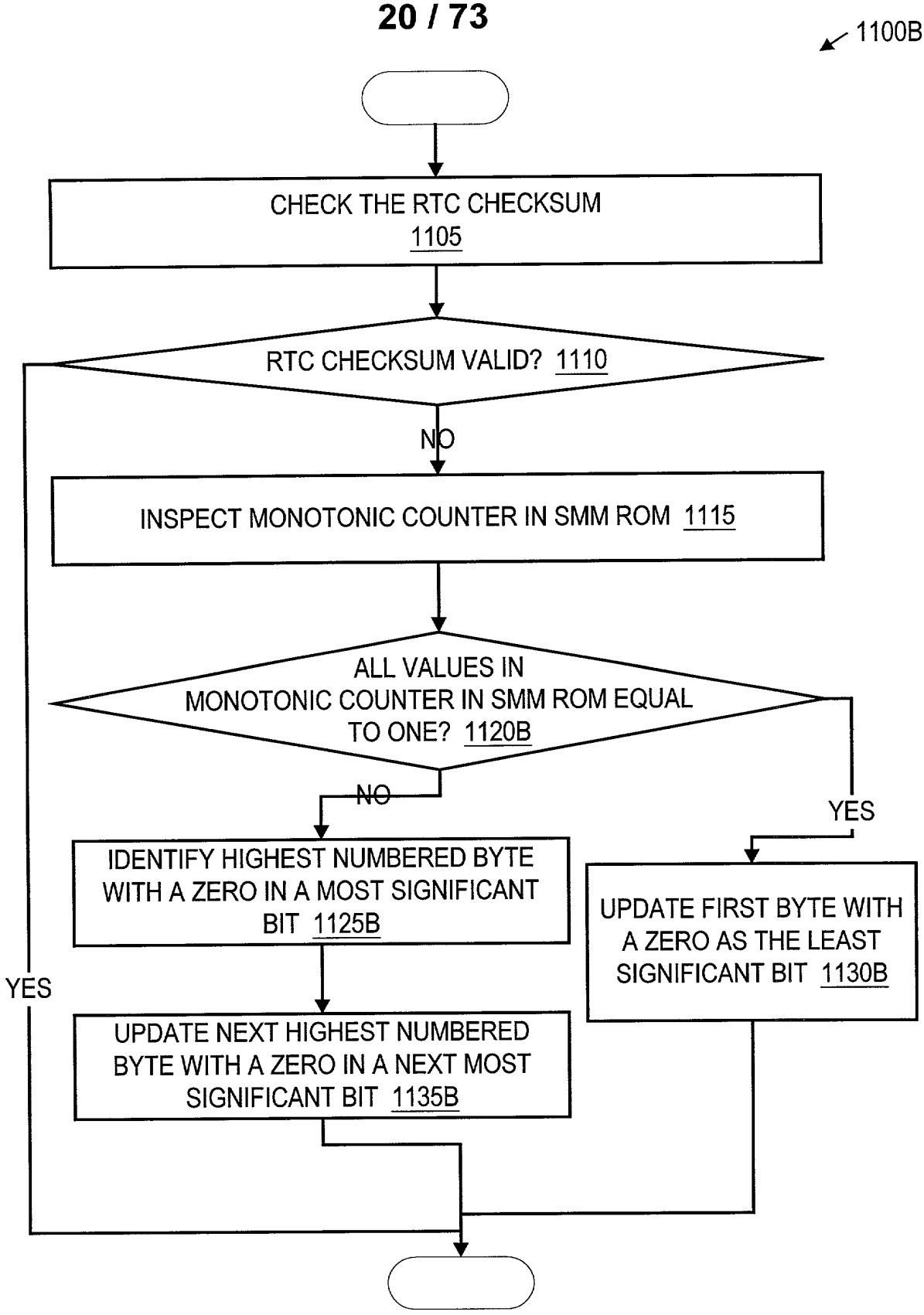
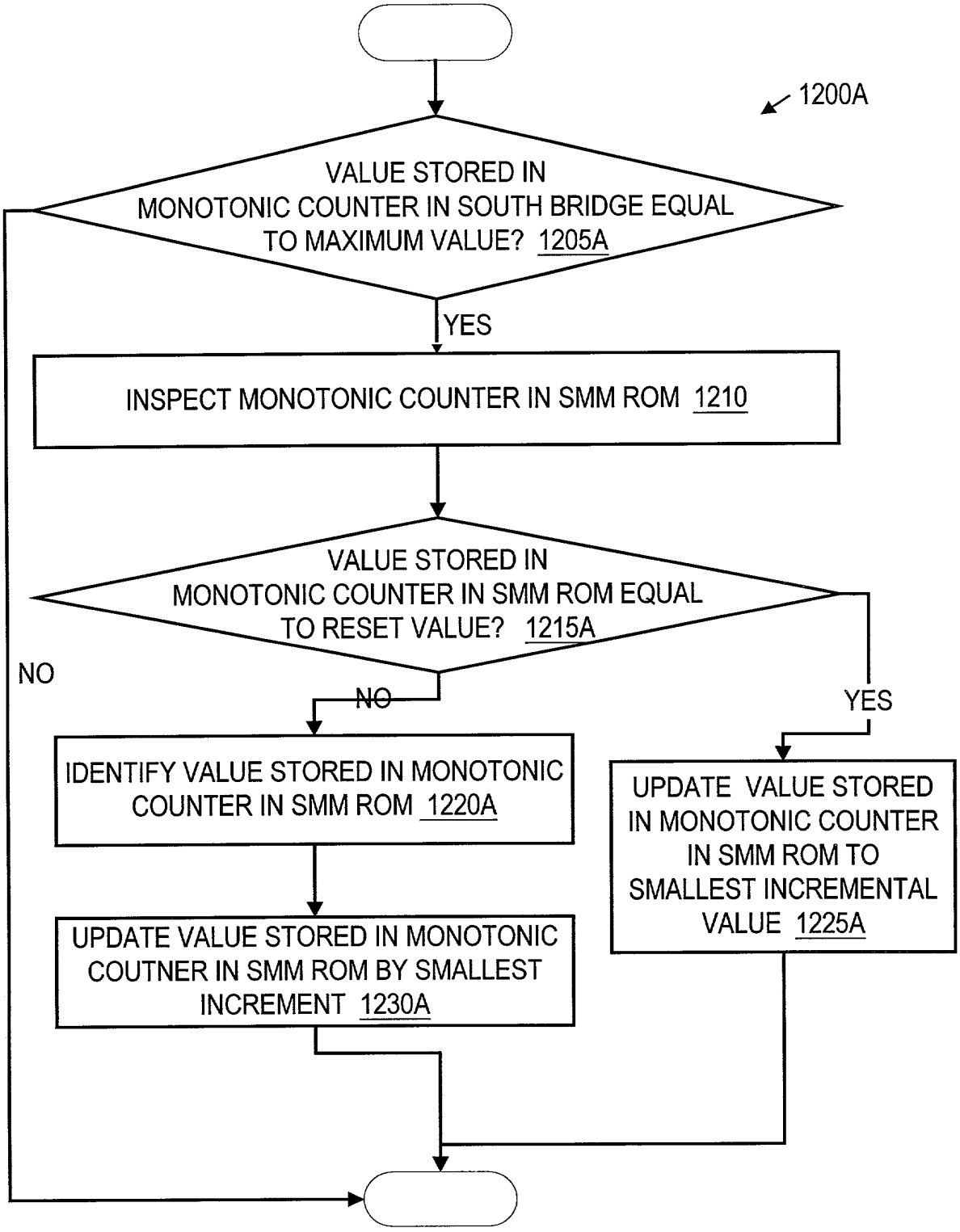

1100B
CHECK THE RTC CHECKSUM 1105
RTC CHECKSUM VALID? 1110
NO
INSPECT MONOTONIC COUNTER IN SMM ROM 1115
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1120B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1125B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1130B
YES
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1135B

Fig. 11B



FIDELITY-1807/3650

Fig. 12A

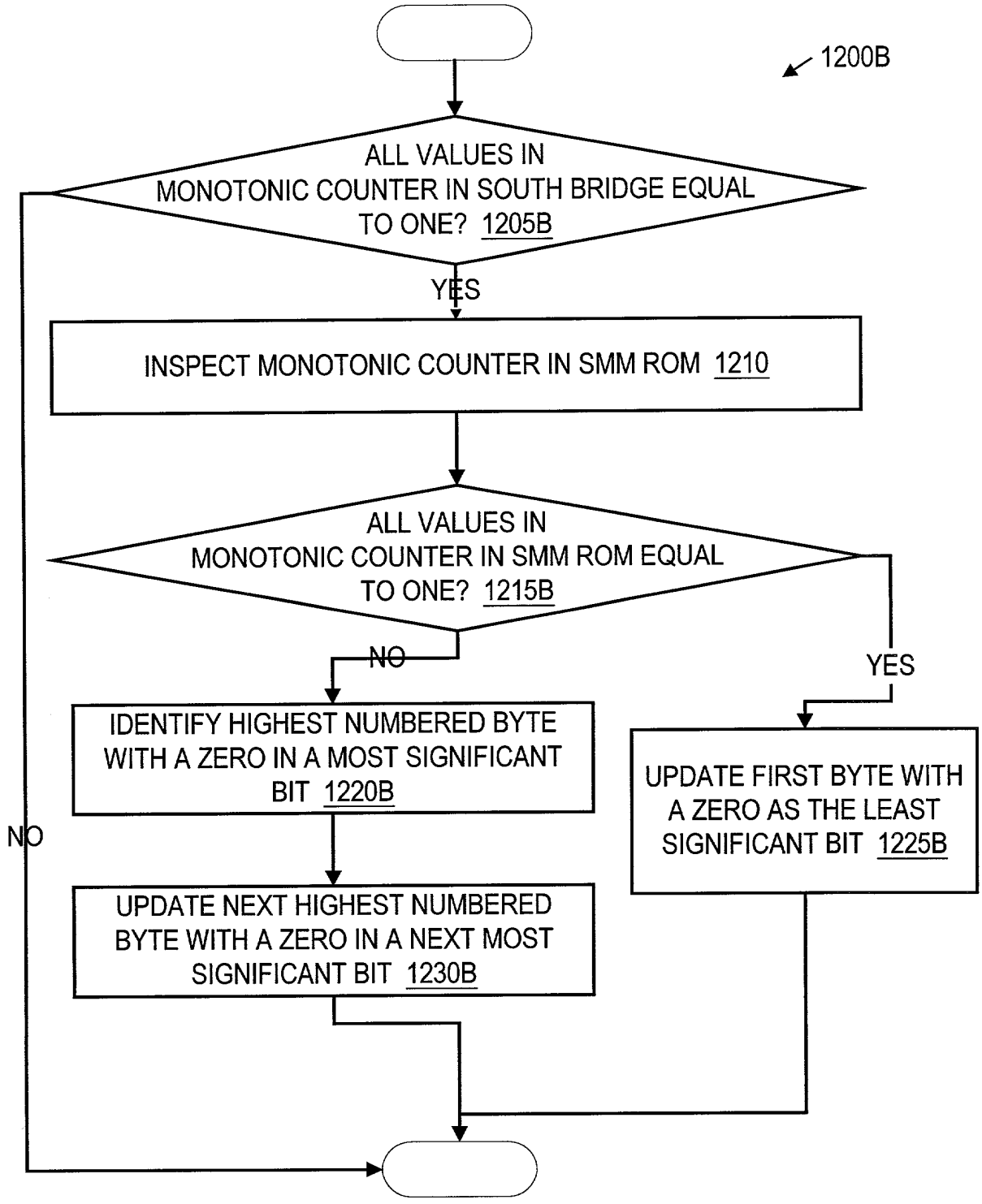

1200B
ALL VALUES IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO ONE? 1205B
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1215B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1220B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1225B
NO
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1230B

Fig. 12B

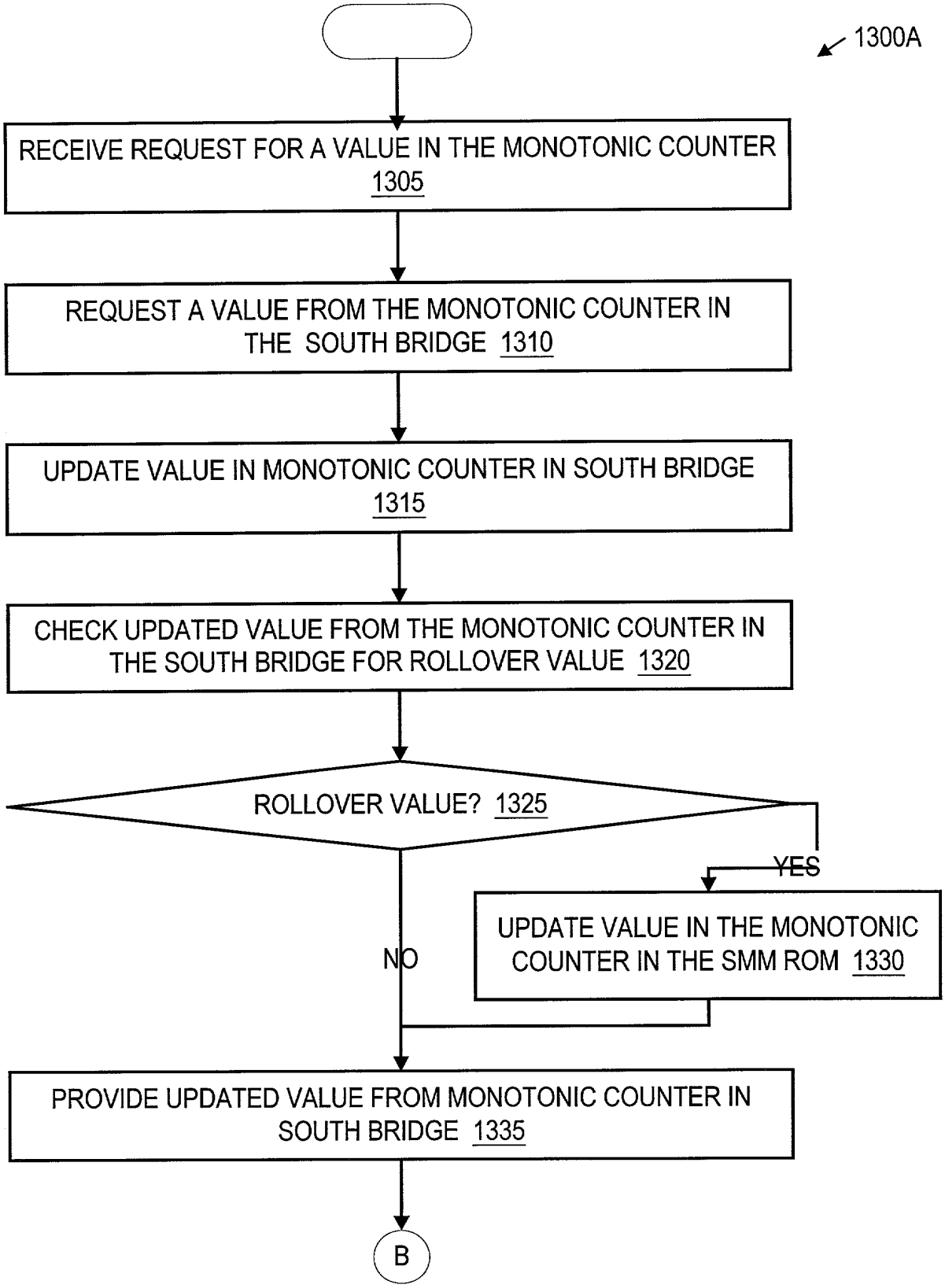


Fig. 13A

FOUNDSTONE-0007463

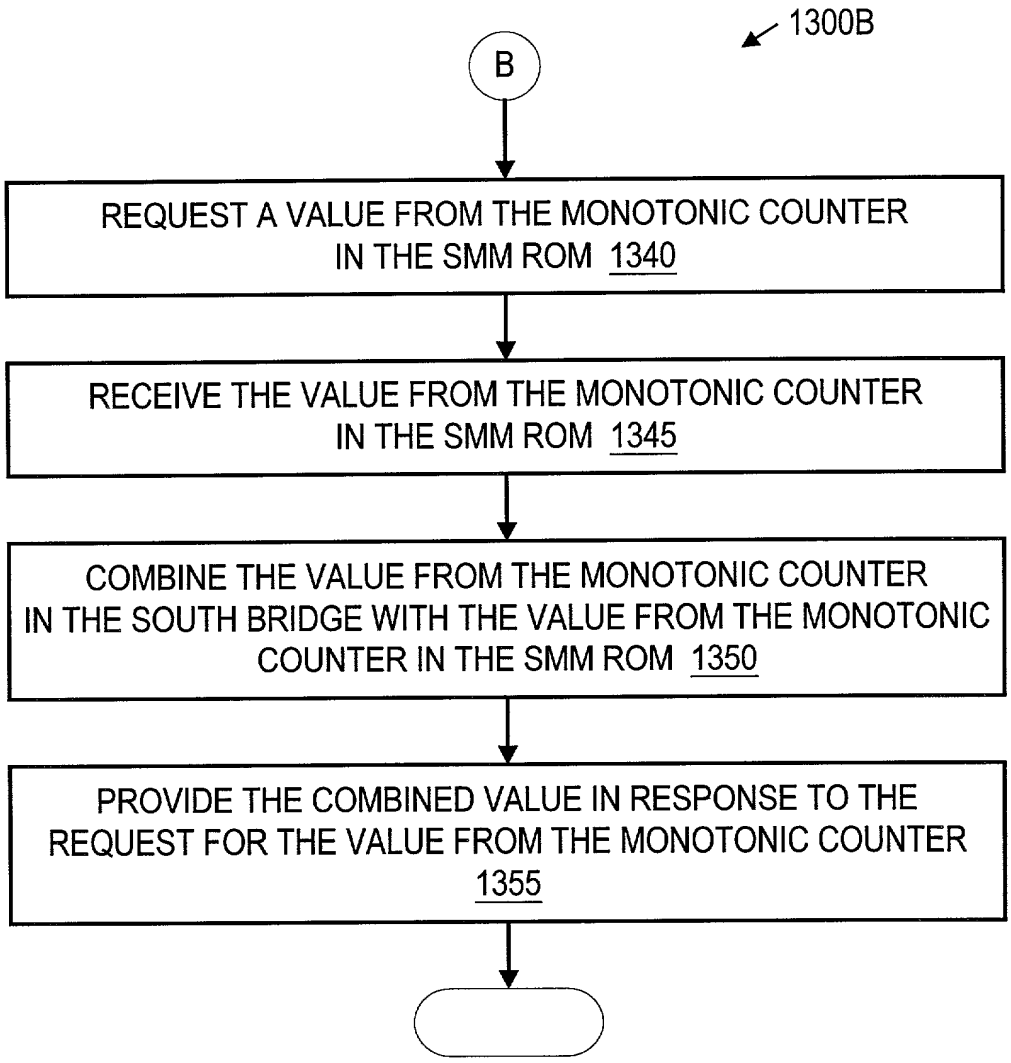

1300B
B
REQUEST A VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1340
RECEIVE THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1345
COMBINE THE VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE WITH THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1350
PROVIDE THE COMBINED VALUE IN RESPONSE TO THE REQUEST FOR THE VALUE FROM THE MONOTONIC COUNTER 1355

Fig. 13B

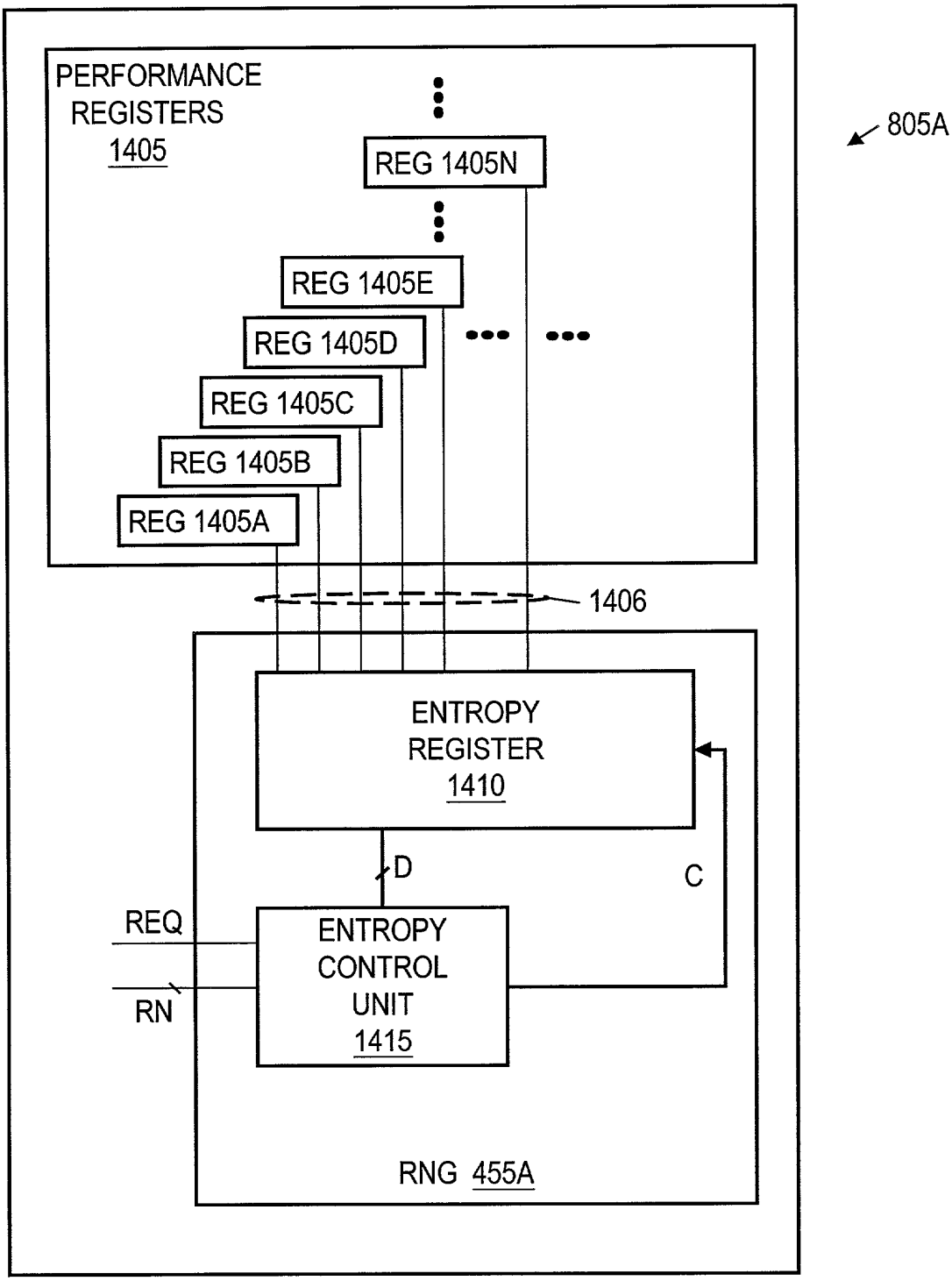

PERFORMANCE
REGISTERS
1405
REG 1405N
REG 1405E
REG 1405D
REG 1405C
REG 1405B
REG 1405A
805A
1406
ENTROPY
REGISTER
1410
D
C
REQ
RN
ENTROPY
CONTROL
UNIT
1415
RNG 455A

Fig. 14A

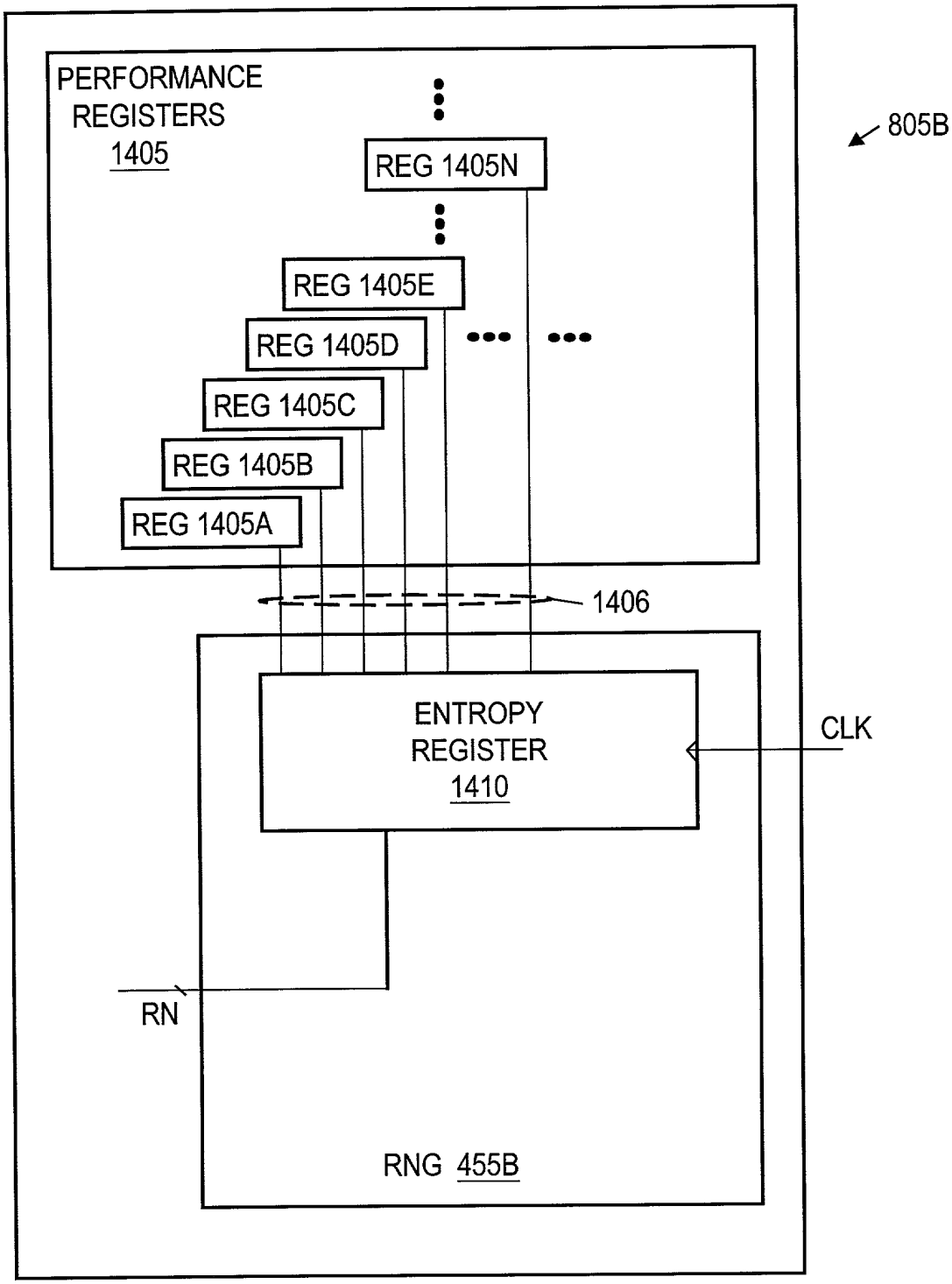


Fig. 14B

FOUNDATION EXHIBIT 2059

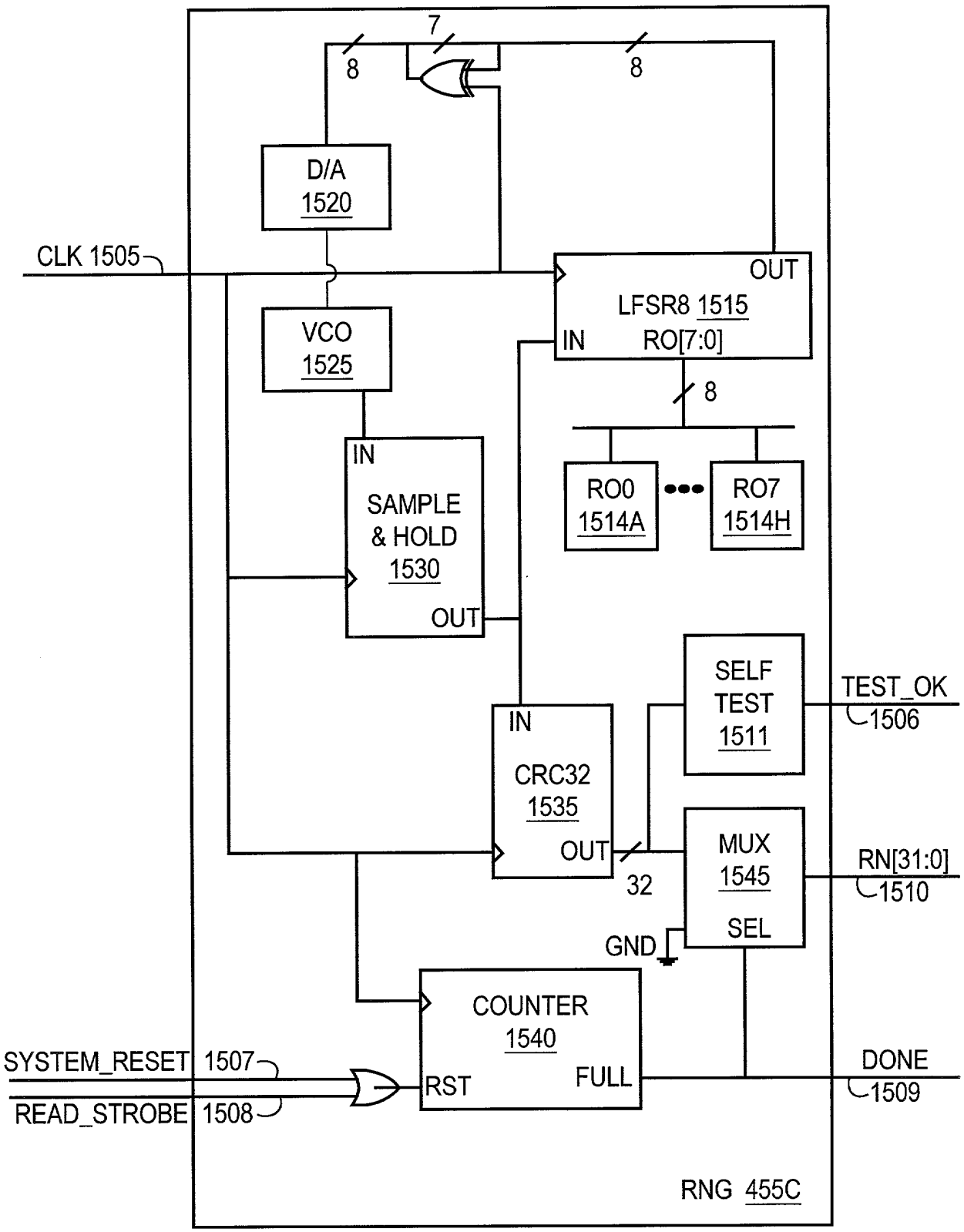

7
8
8
D/A
1520
CLK 1505
OUT
LFSR8 1515
IN
RO[7:0]
VCO
1525
8
IN
SAMPLE
& HOLD
1530
OUT
RO0
1514A
RO7
1514H
SELF
TEST
1511
TEST_OK
1506
IN
CRC32
1535
OUT
32
MUX
1545
SEL
RN[31:0]
1510
GND
COUNTER
1540
SYSTEM_RESET 1507
READ_STROBE 1508
RST
FULL
DONE
1509
RNG 455C

Fig. 15

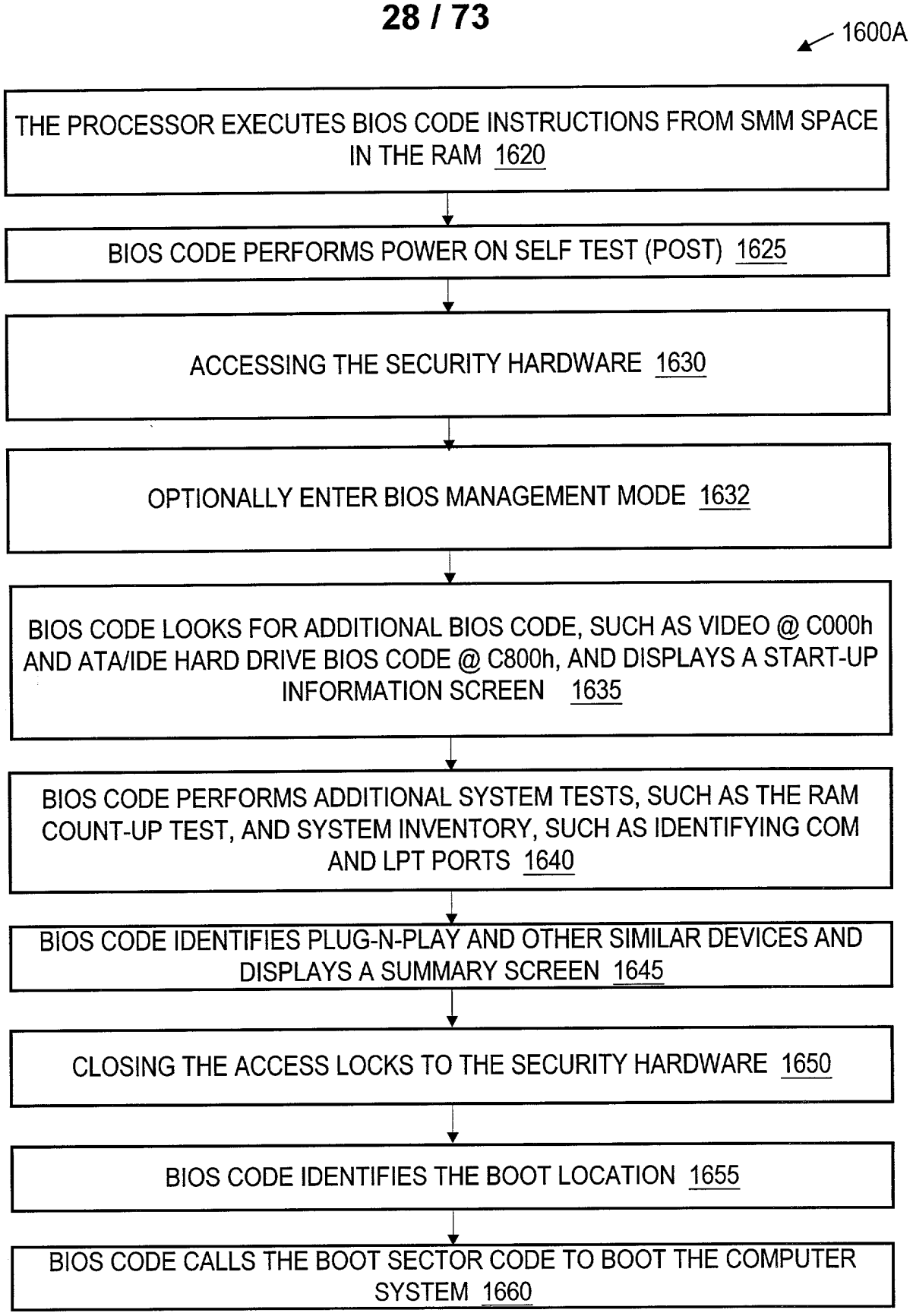
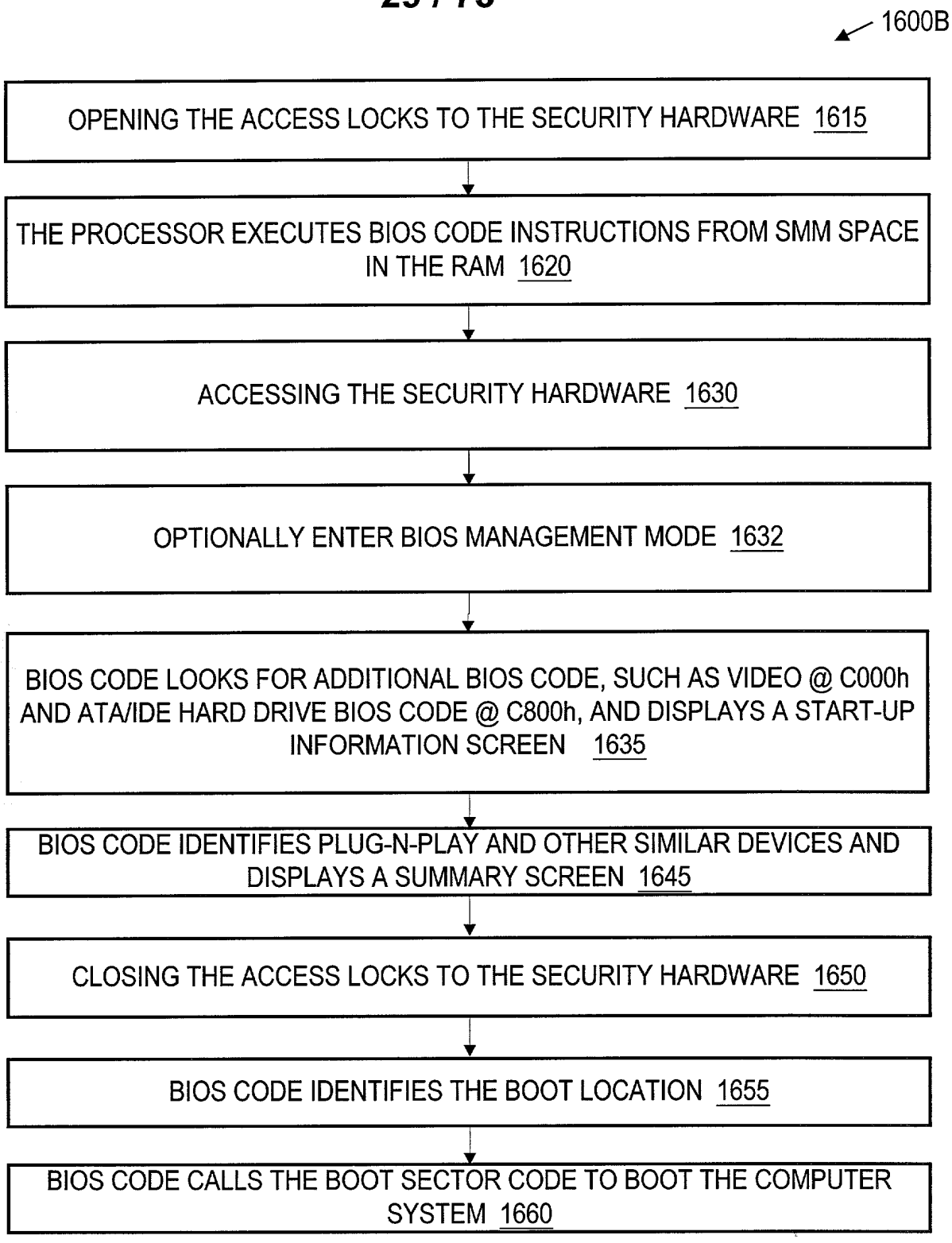
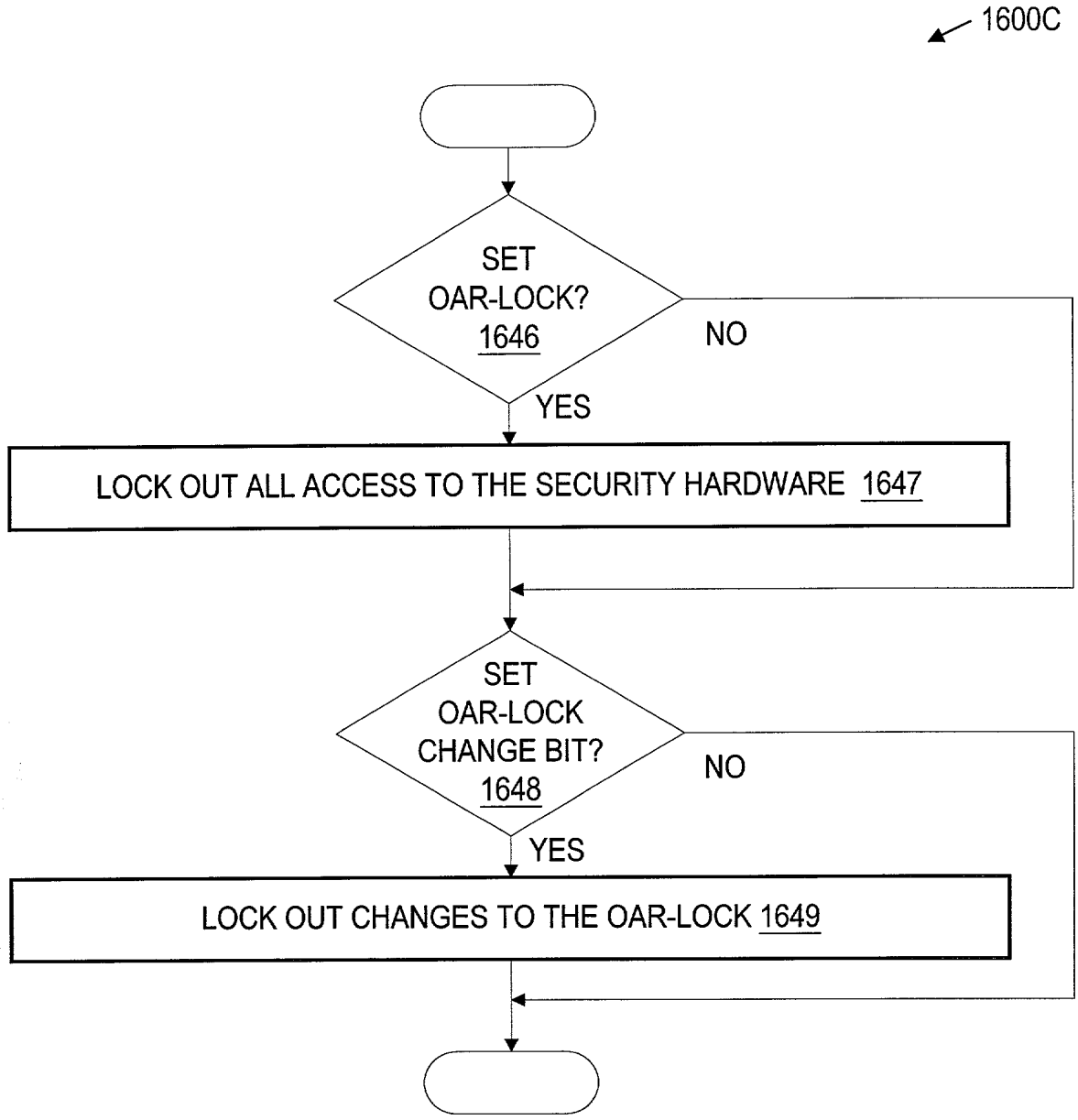

1600A
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
BIOS CODE PERFORMS POWER ON SELF TEST (POST) 1625
ACCESSING THE SECURITY HARDWARE 1630
OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635
BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 1640
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
BIOS CODE IDENTIFIES THE BOOT LOCATION 1655
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16A



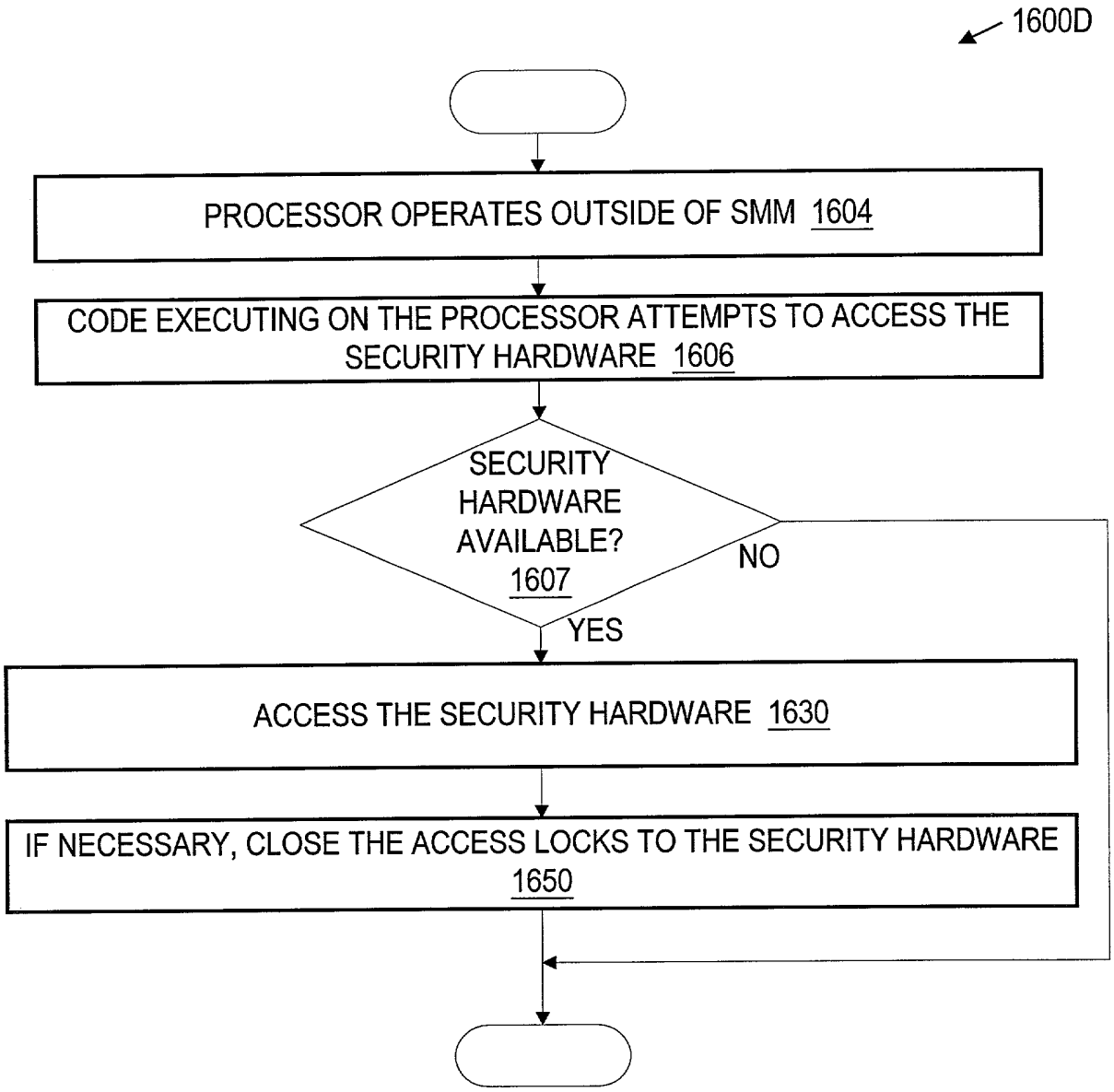
T0065D "1801F7860

Fig. 16B



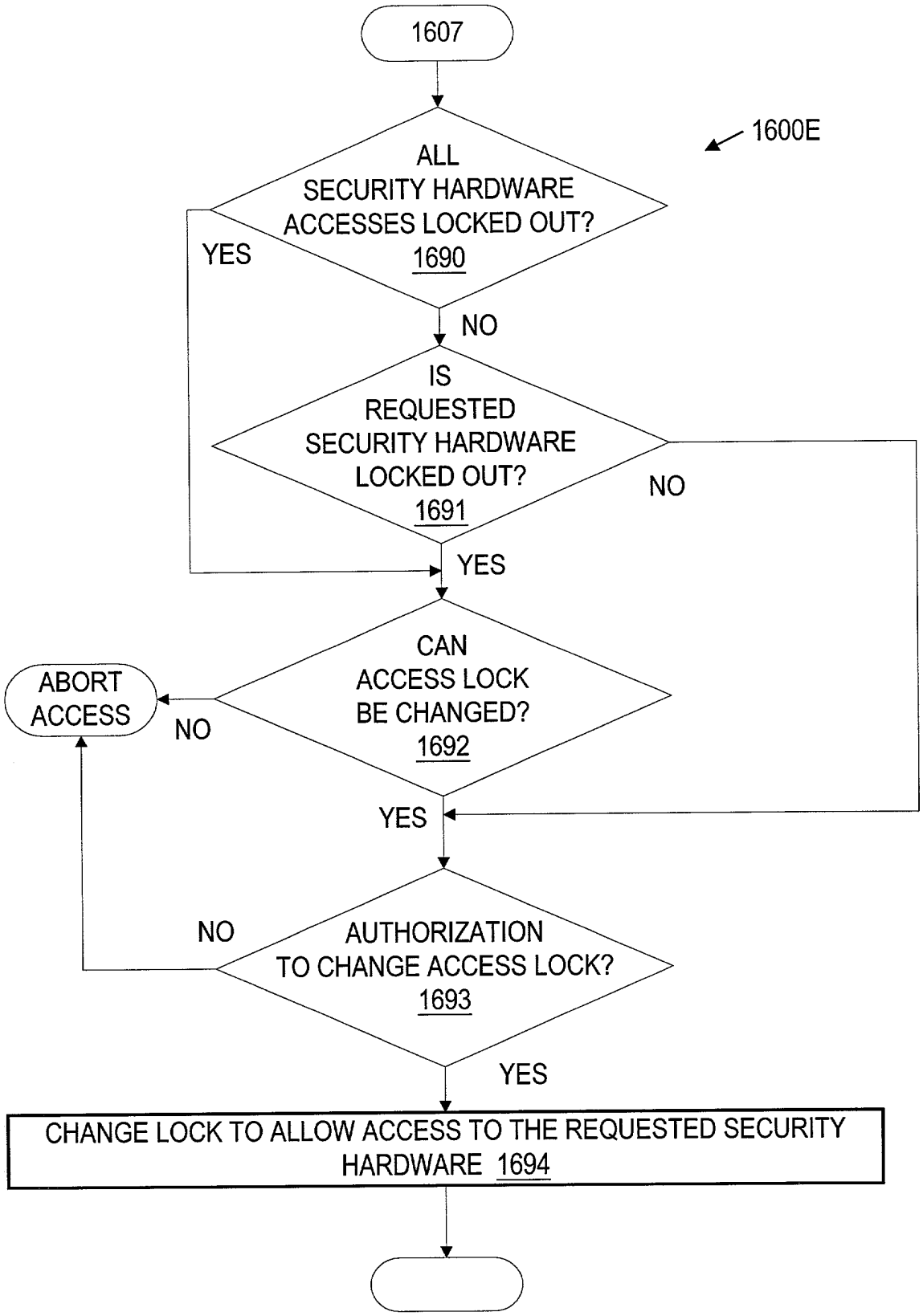
T0056504900F7960

Fig. 16C



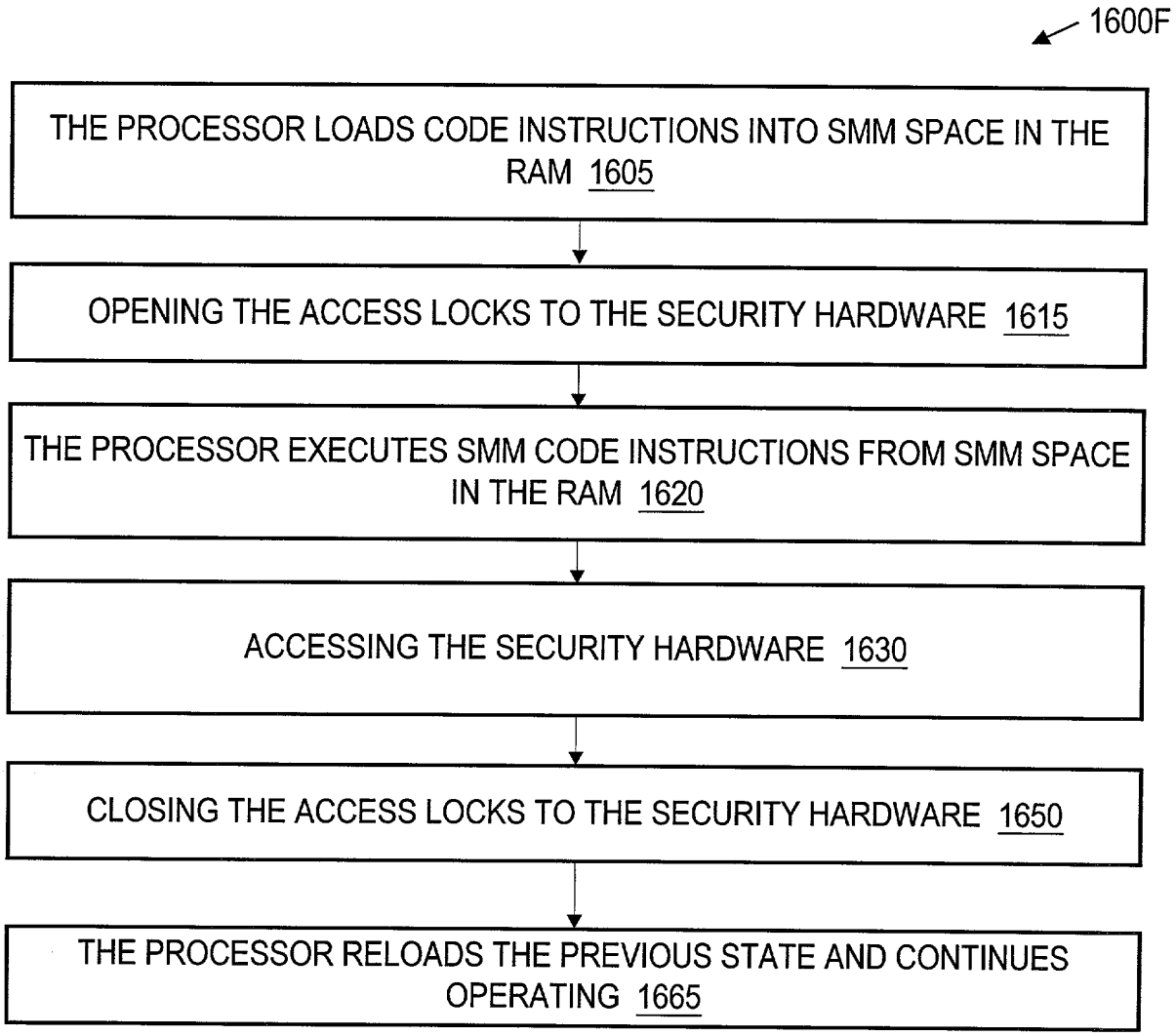
0987654321 - 0987654321

Fig. 16D



1600E-1600E-1690-1691-1692-1693-1694

Fig. 16E



1005250-1504709.pdf

Fig. 16F

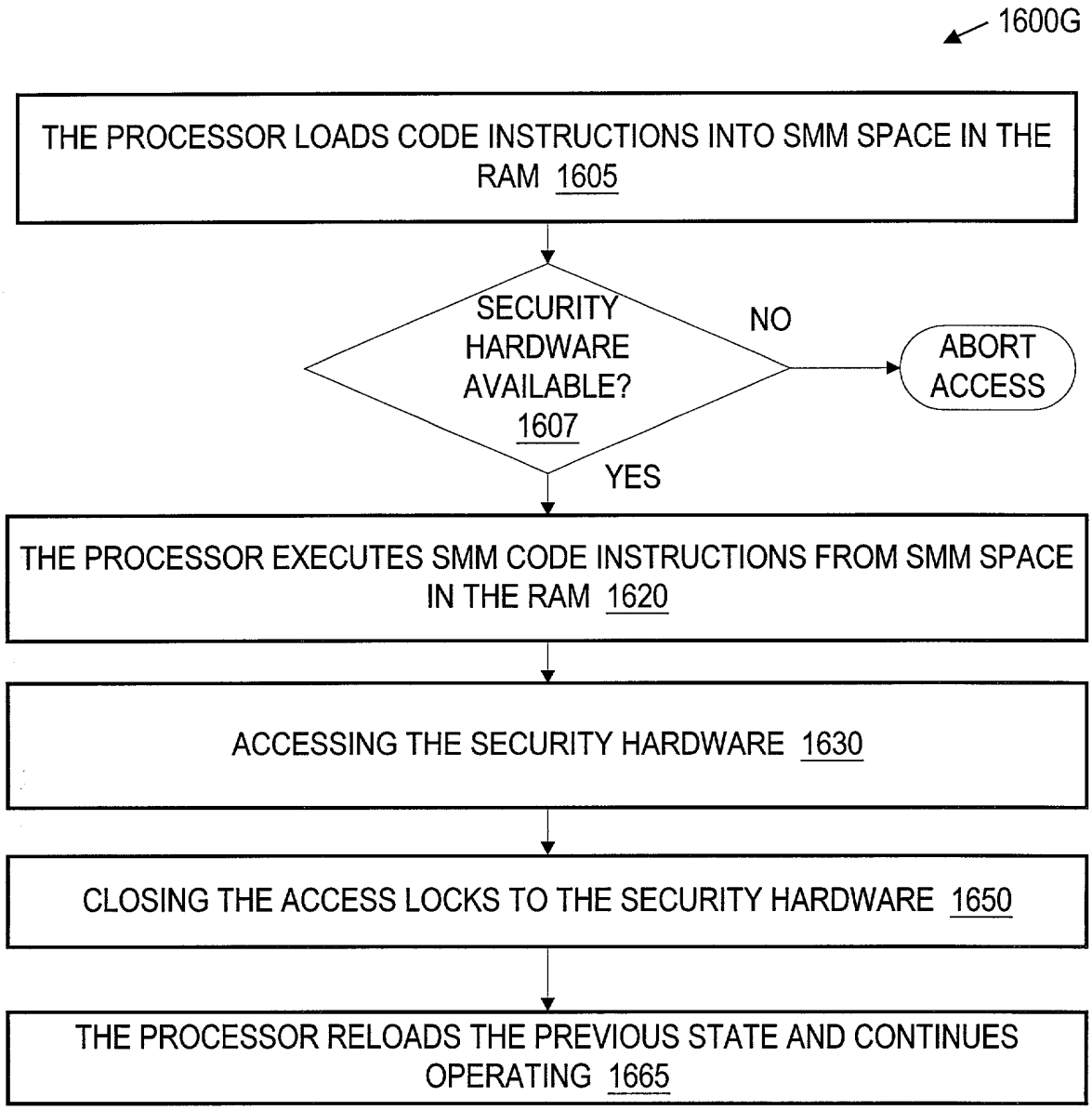


EXHIBIT 1008 - 0569 of 0598

Fig. 16G

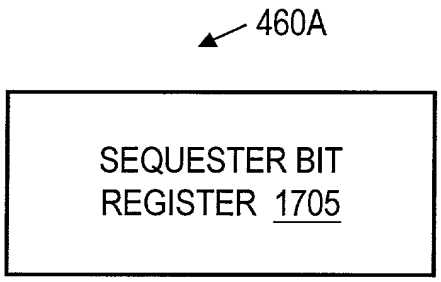


Fig. 17A

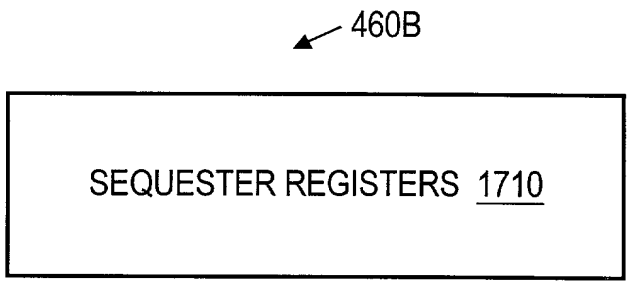


Fig. 17B

TOSE50-1301-73650

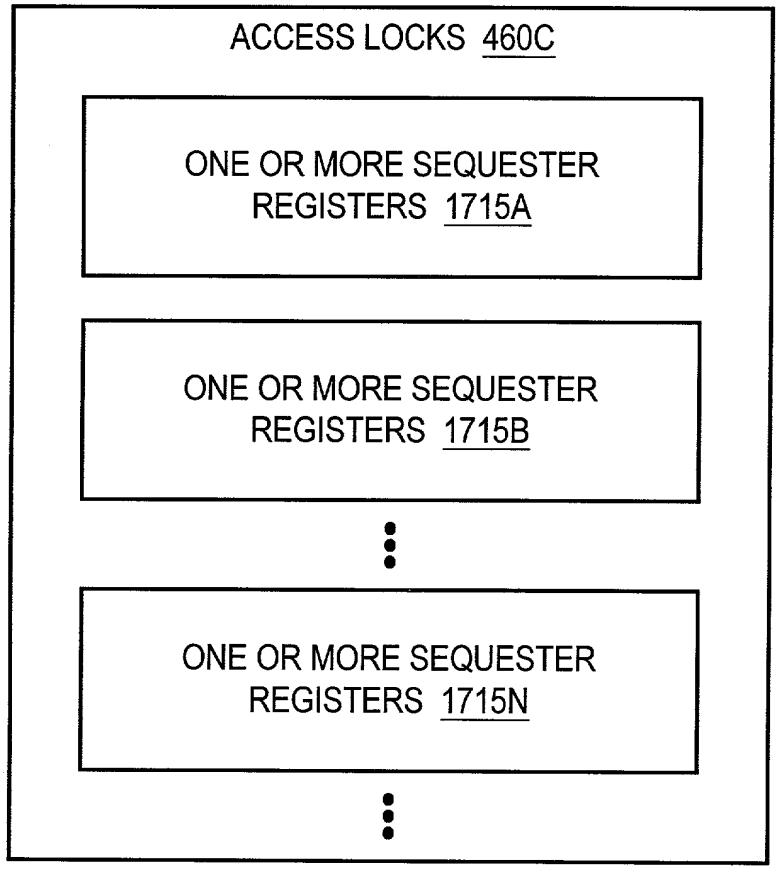


Fig. 17C

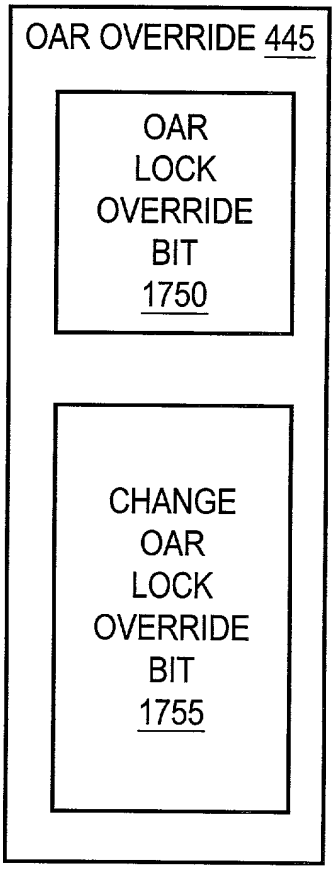


Fig. 17D

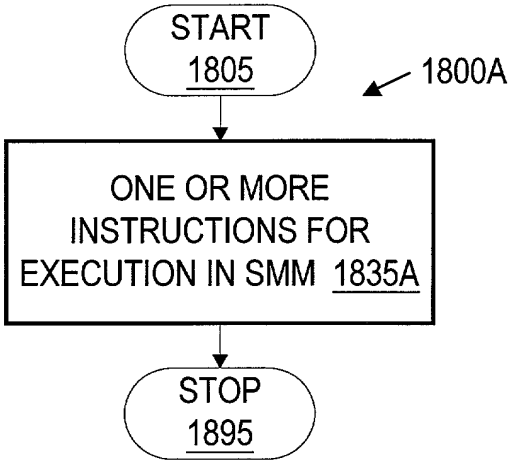


Fig. 18A
PRIOR ART

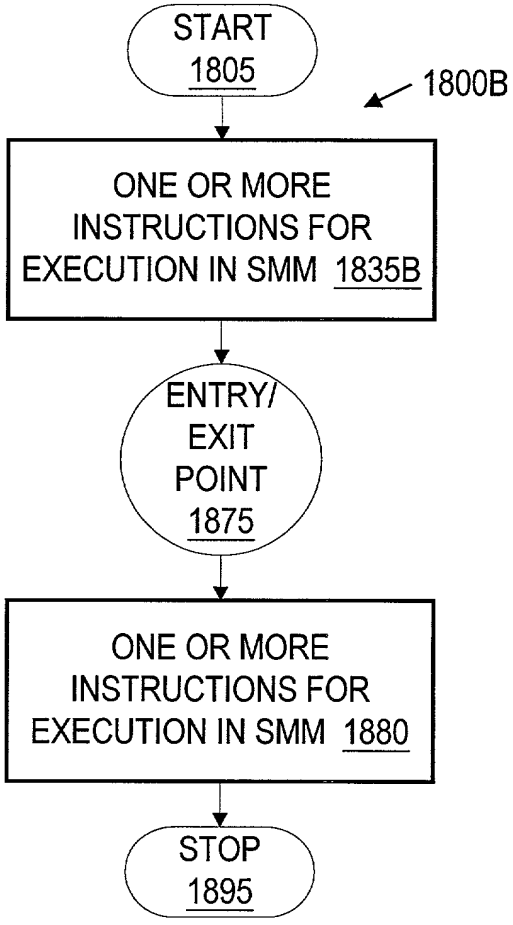


Fig. 18B

Tobacco Exhibit 2060

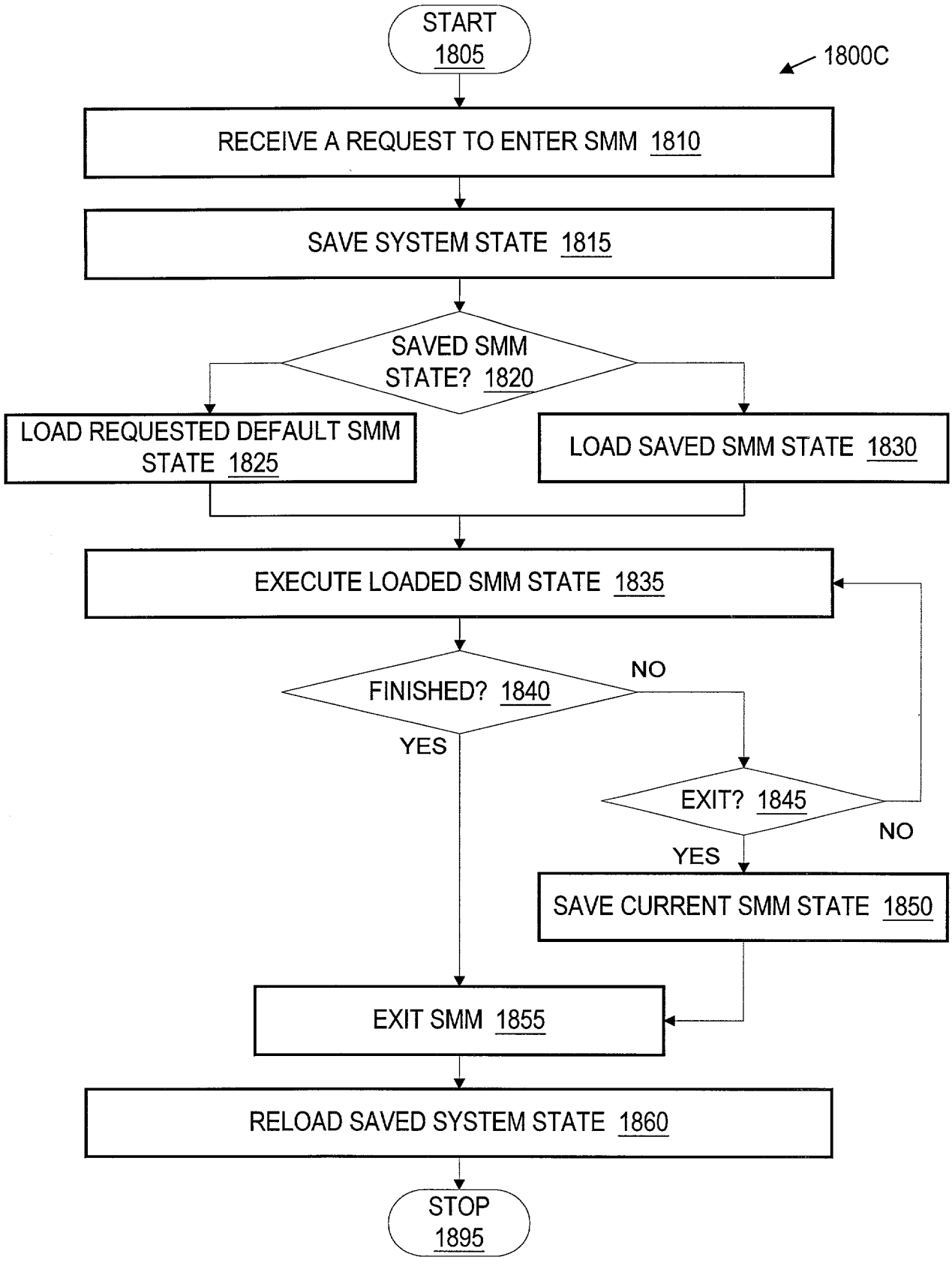
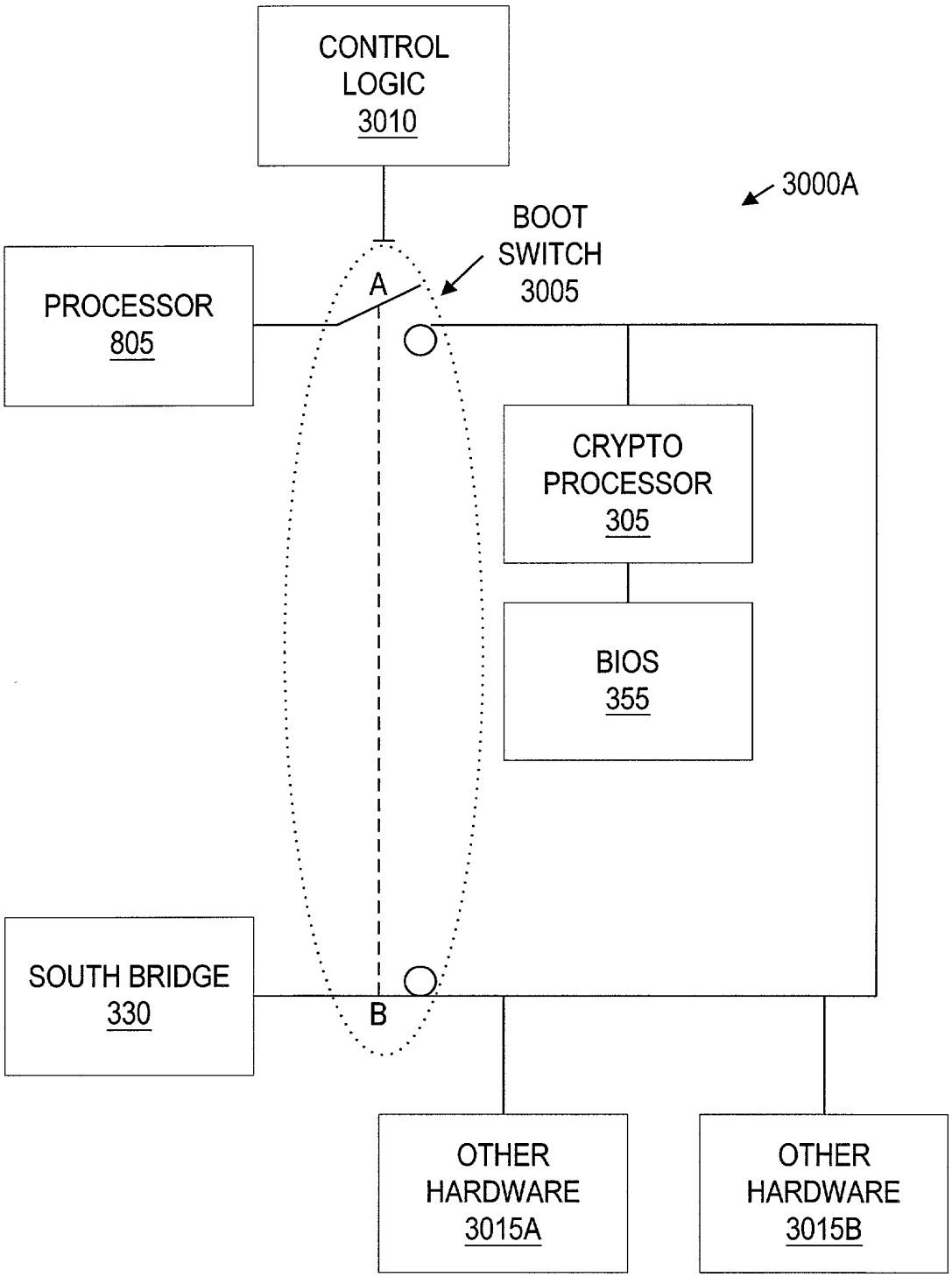

START 1805
1800C
RECEIVE A REQUEST TO ENTER SMM 1810
SAVE SYSTEM STATE 1815
SAVED SMM STATE? 1820
LOAD REQUESTED DEFAULT SMM STATE 1825
LOAD SAVED SMM STATE 1830
EXECUTE LOADED SMM STATE 1835
FINISHED? 1840
NO
YES
EXIT? 1845
NO
YES
SAVE CURRENT SMM STATE 1850
EXIT SMM 1855
RELOAD SAVED SYSTEM STATE 1860
STOP 1895

Fig. 18C



09571064 - 053007

Fig. 19A

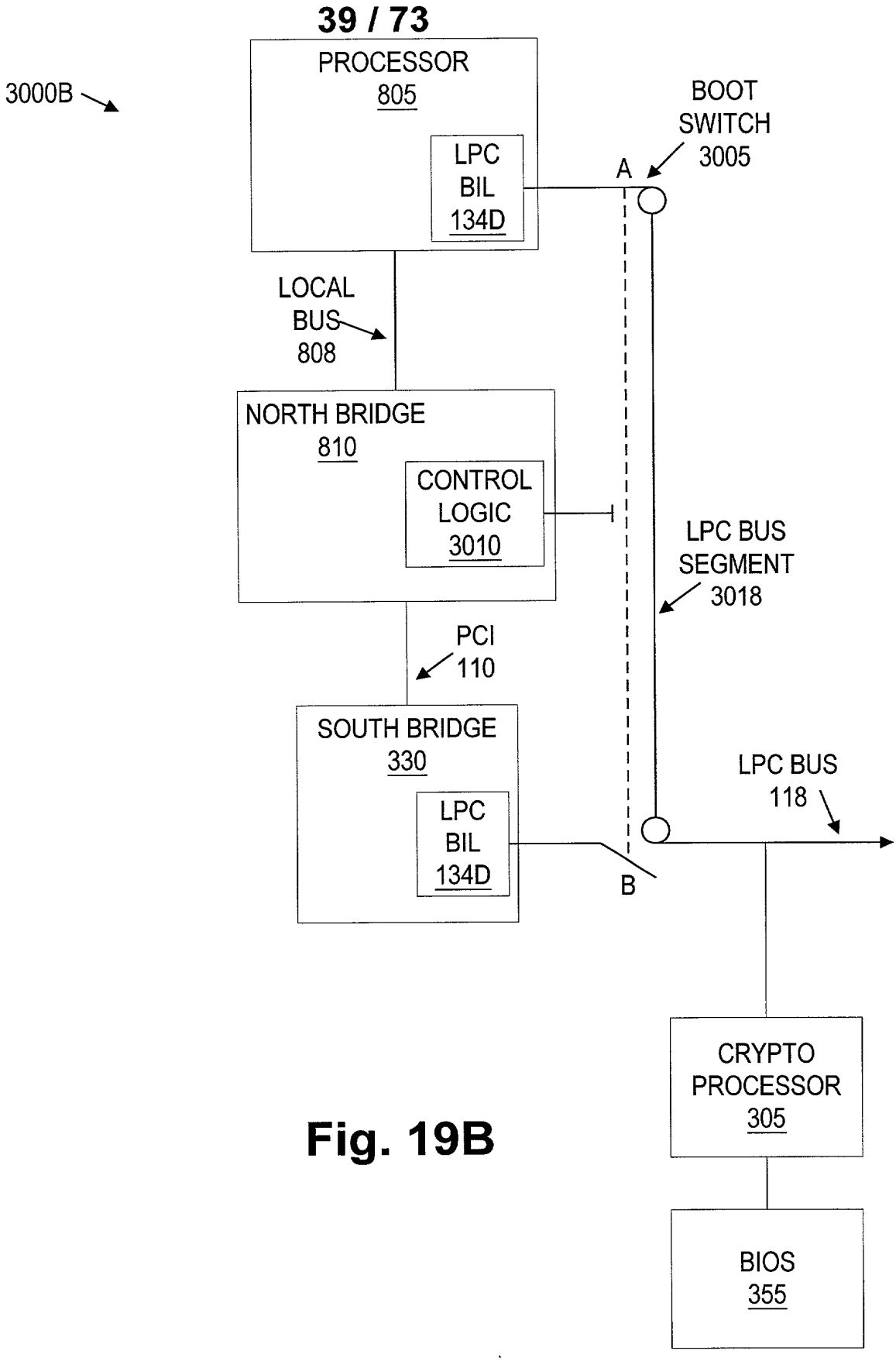
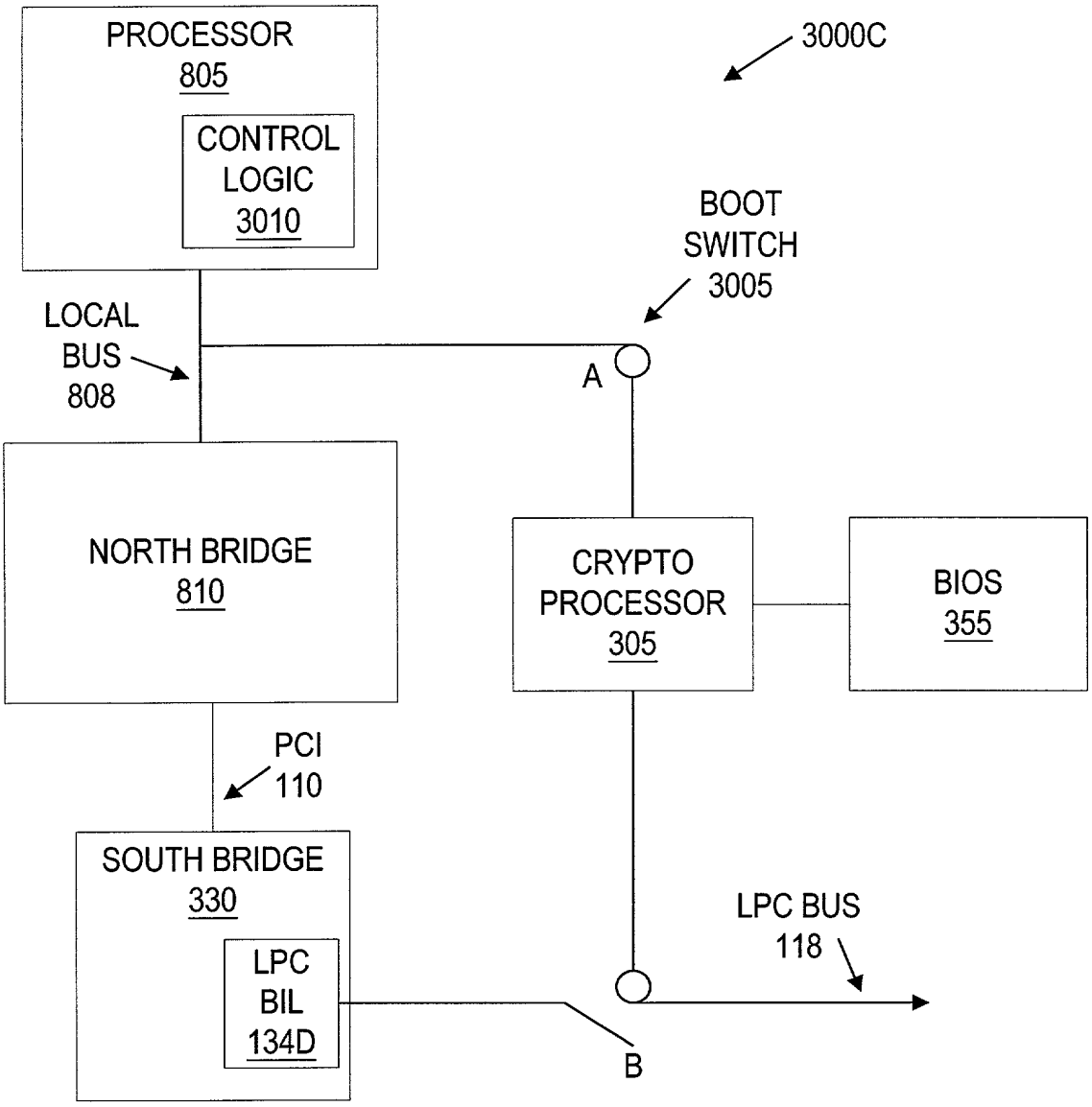


Fig. 19B

FOOTER-1801-7650



TOSEQ-4301/650

Fig. 19C

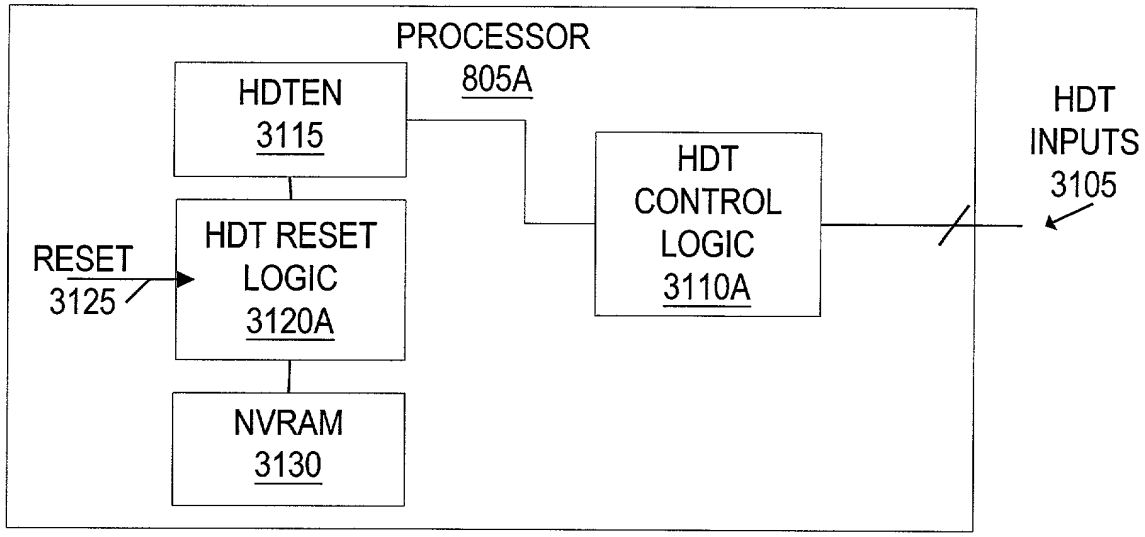


Fig. 20A

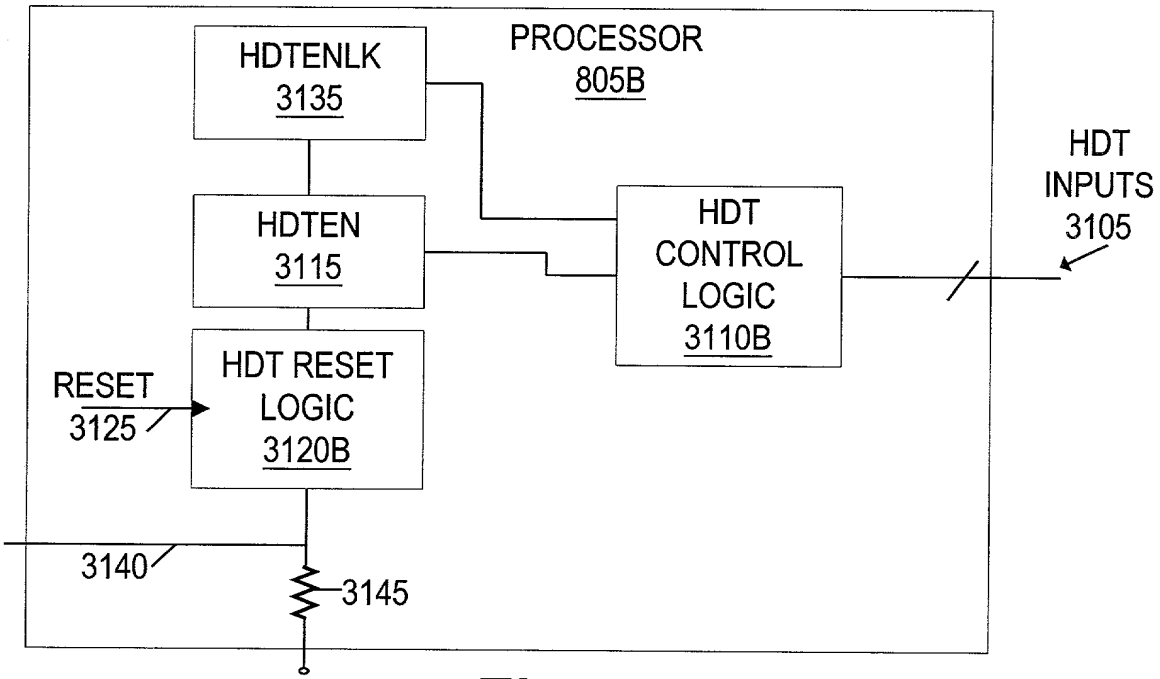


Fig. 20B

FOUR50 + 801/3660

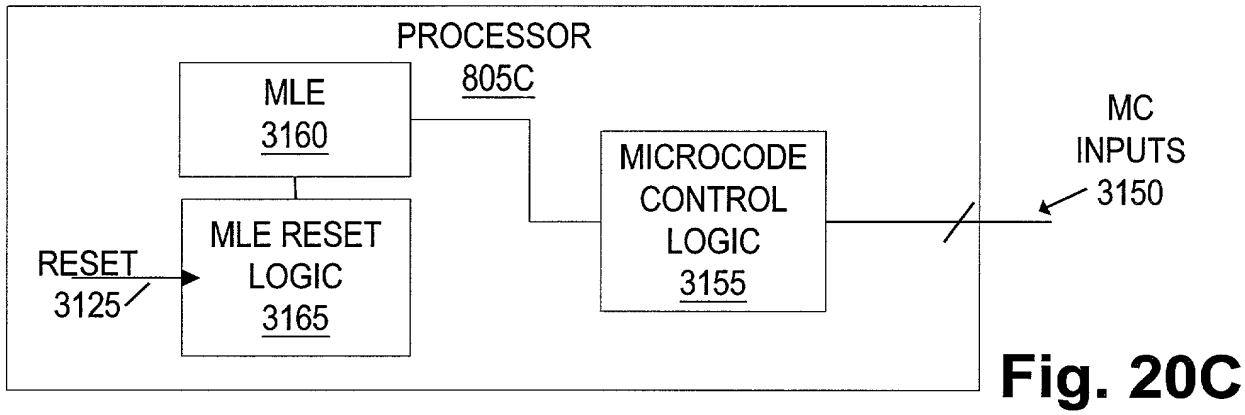


Fig. 20C

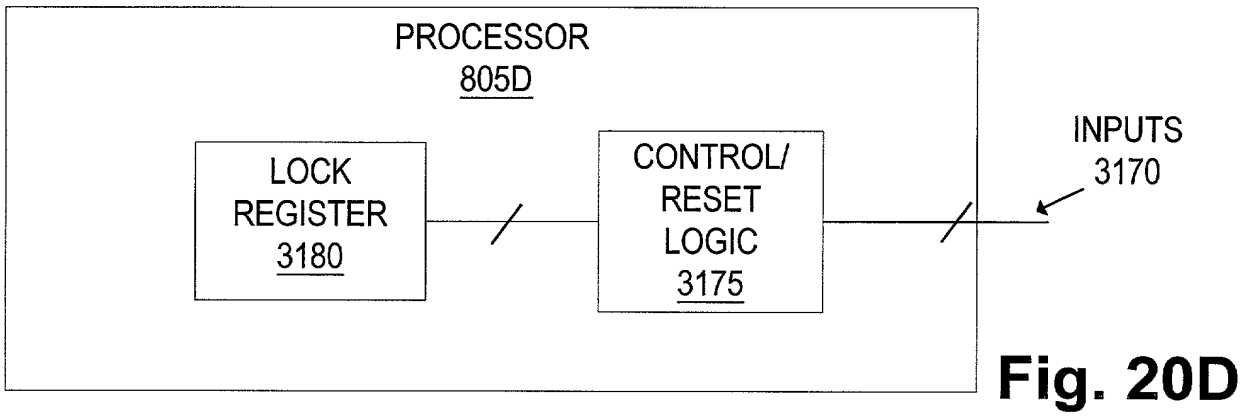


Fig. 20D

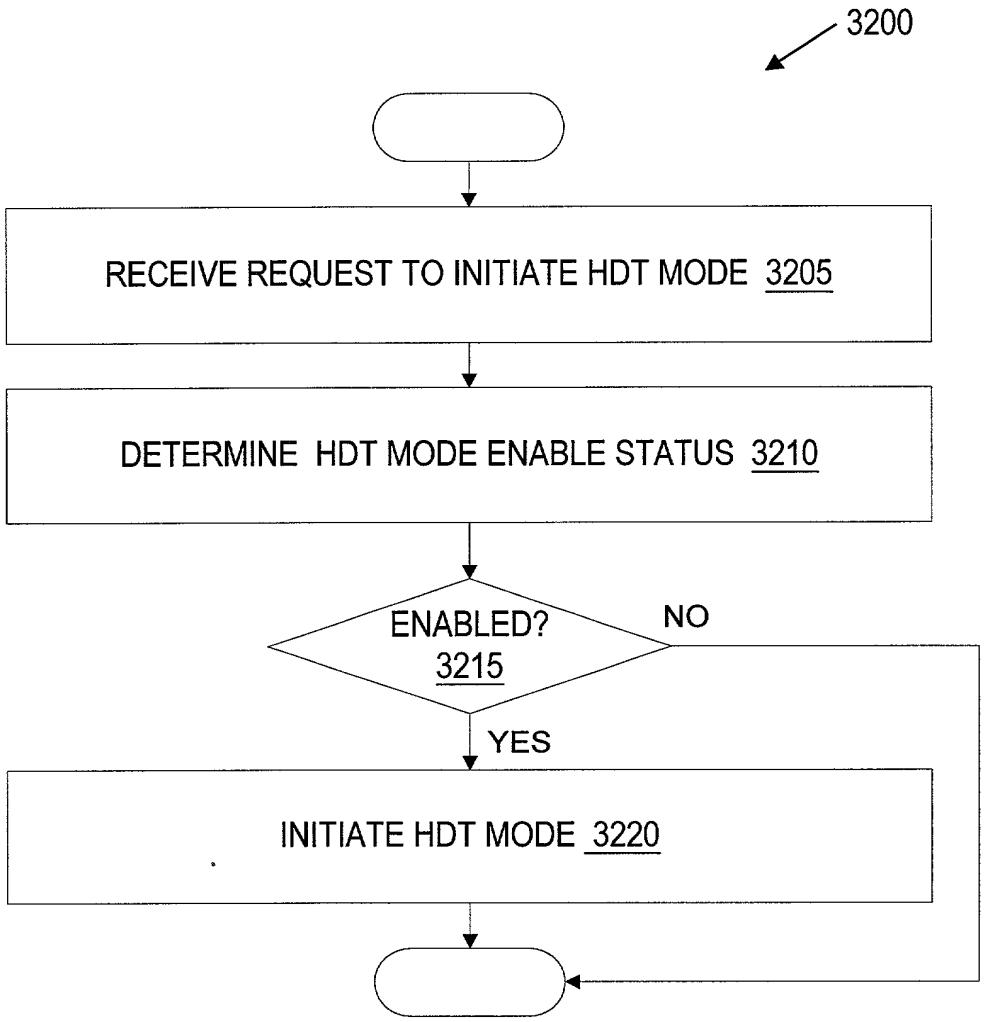


Fig. 21

FOSS-00076

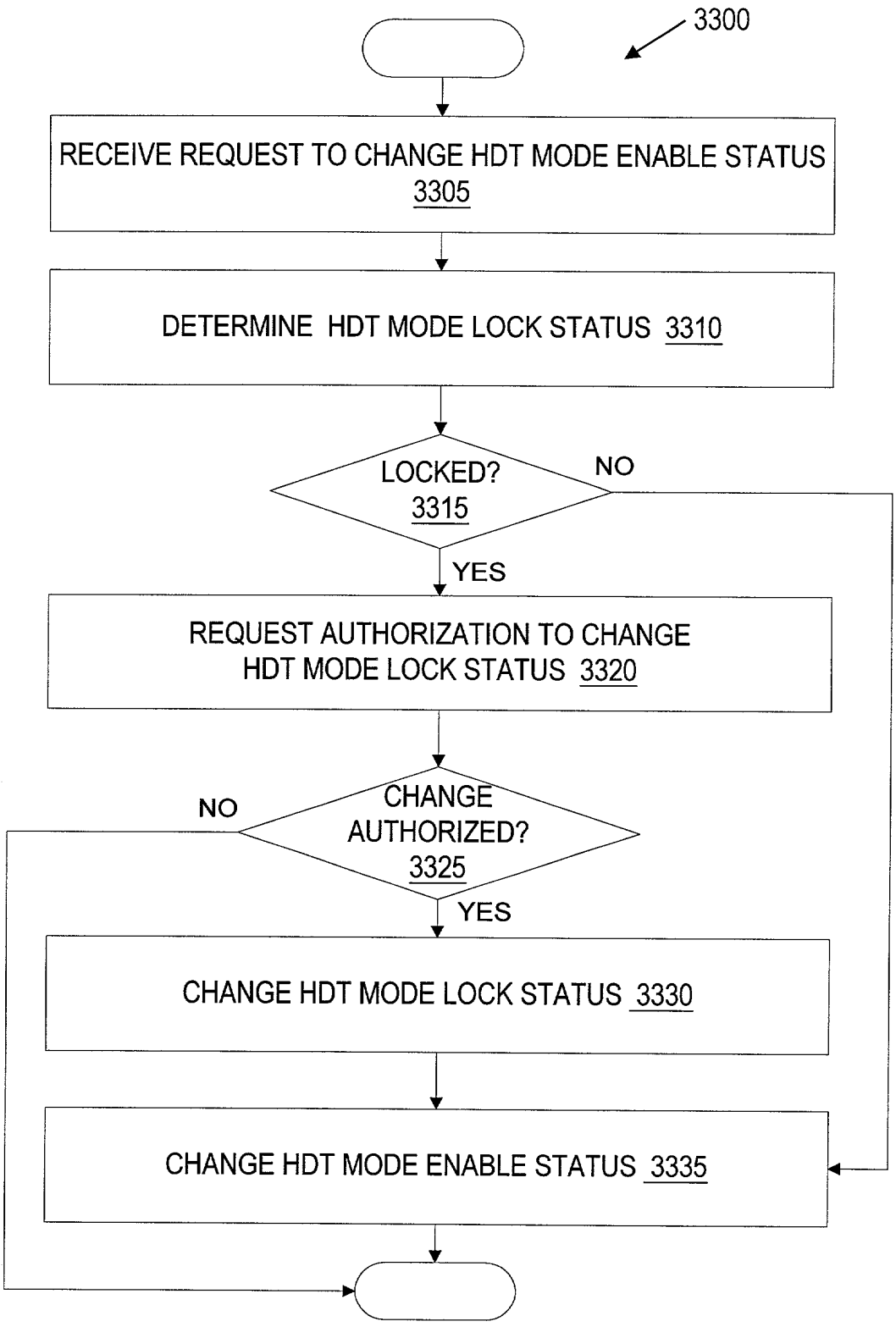

3300
RECEIVE REQUEST TO CHANGE HDT MODE ENABLE STATUS 3305
DETERMINE HDT MODE LOCK STATUS 3310
LOCKED? 3315
NO
YES
REQUEST AUTHORIZATION TO CHANGE HDT MODE LOCK STATUS 3320
CHANGE AUTHORIZED? 3325
NO
YES
CHANGE HDT MODE LOCK STATUS 3330
CHANGE HDT MODE ENABLE STATUS 3335

Fig. 22

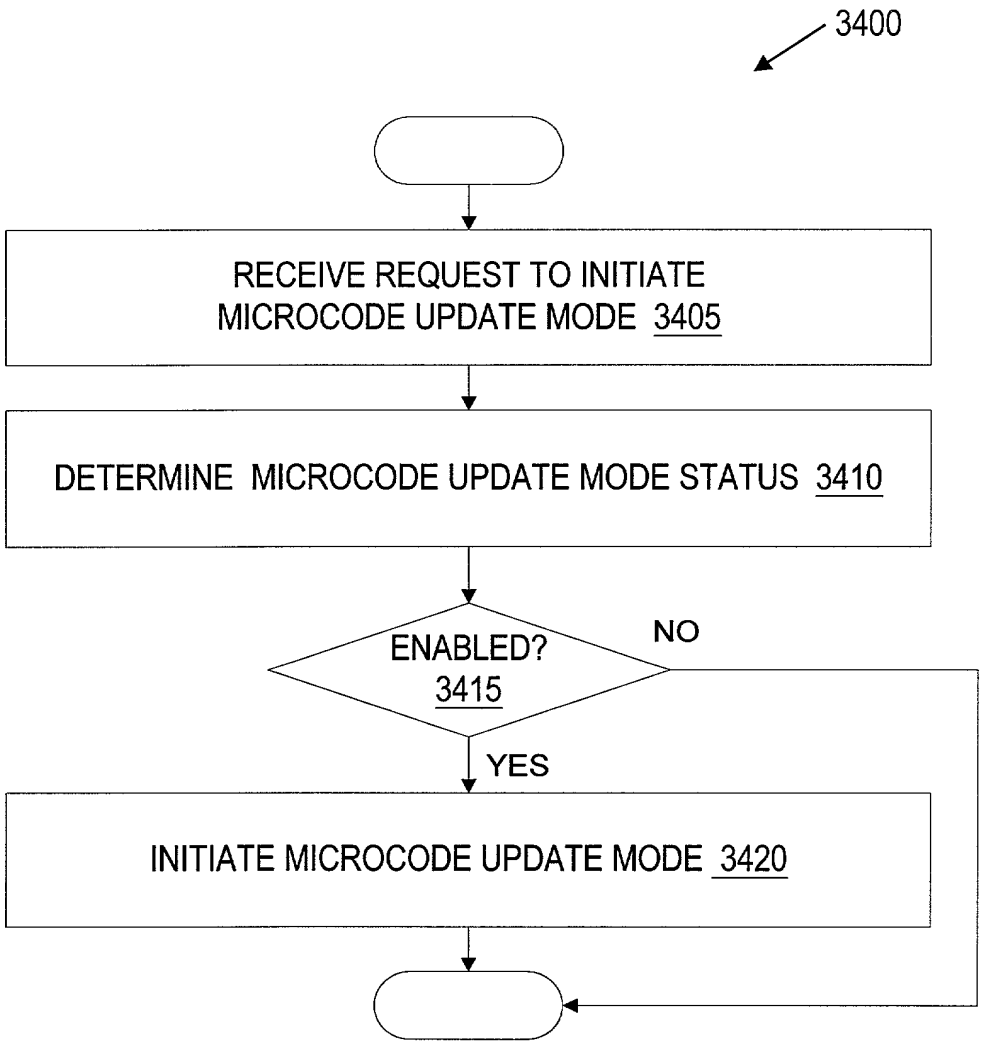


Fig. 23

FOR 2550-4600 / 3650

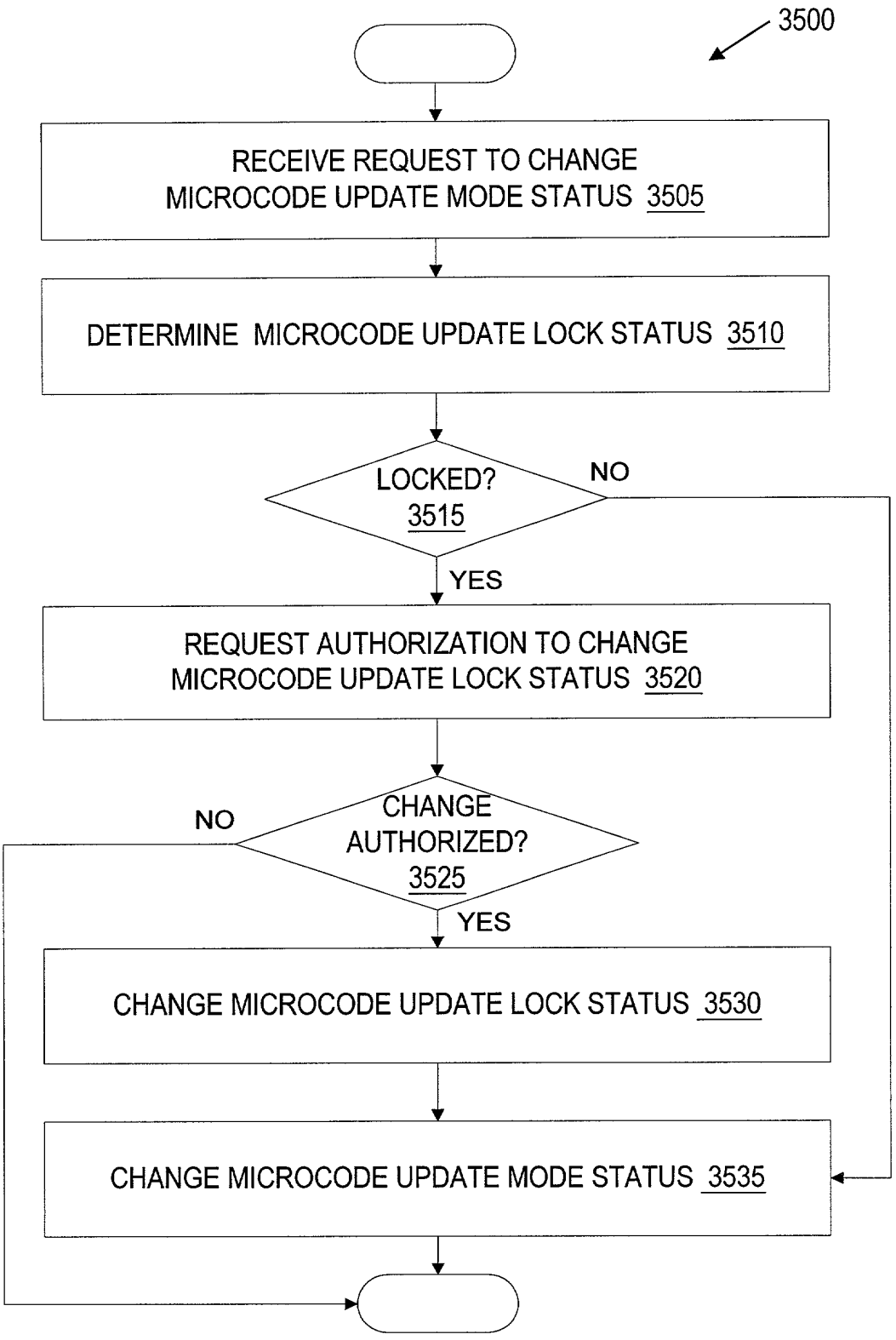

3500
RECEIVE REQUEST TO CHANGE MICROCODE UPDATE MODE STATUS 3505
DETERMINE MICROCODE UPDATE LOCK STATUS 3510
LOCKED? 3515
NO
YES
REQUEST AUTHORIZATION TO CHANGE MICROCODE UPDATE LOCK STATUS 3520
CHANGE AUTHORIZED? 3525
NO
YES
CHANGE MICROCODE UPDATE LOCK STATUS 3530
CHANGE MICROCODE UPDATE MODE STATUS 3535

Fig. 24

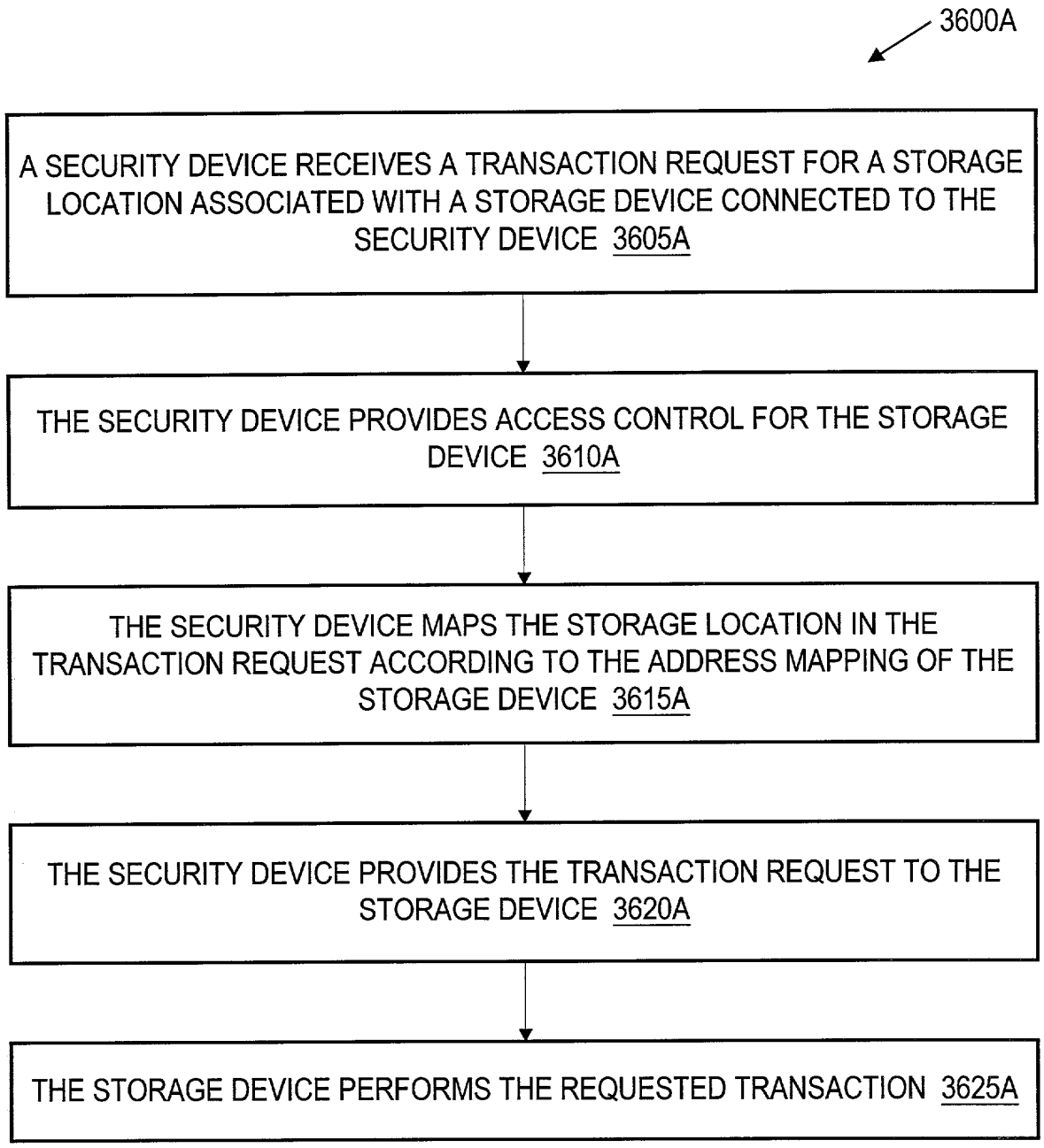

3600A
A SECURITY DEVICE RECEIVES A TRANSACTION REQUEST FOR A STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3605A
THE SECURITY DEVICE PROVIDES ACCESS CONTROL FOR THE STORAGE DEVICE 3610A
THE SECURITY DEVICE MAPS THE STORAGE LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE STORAGE DEVICE 3615A
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3620A
THE STORAGE DEVICE PERFORMS THE REQUESTED TRANSACTION 3625A

Fig. 25A

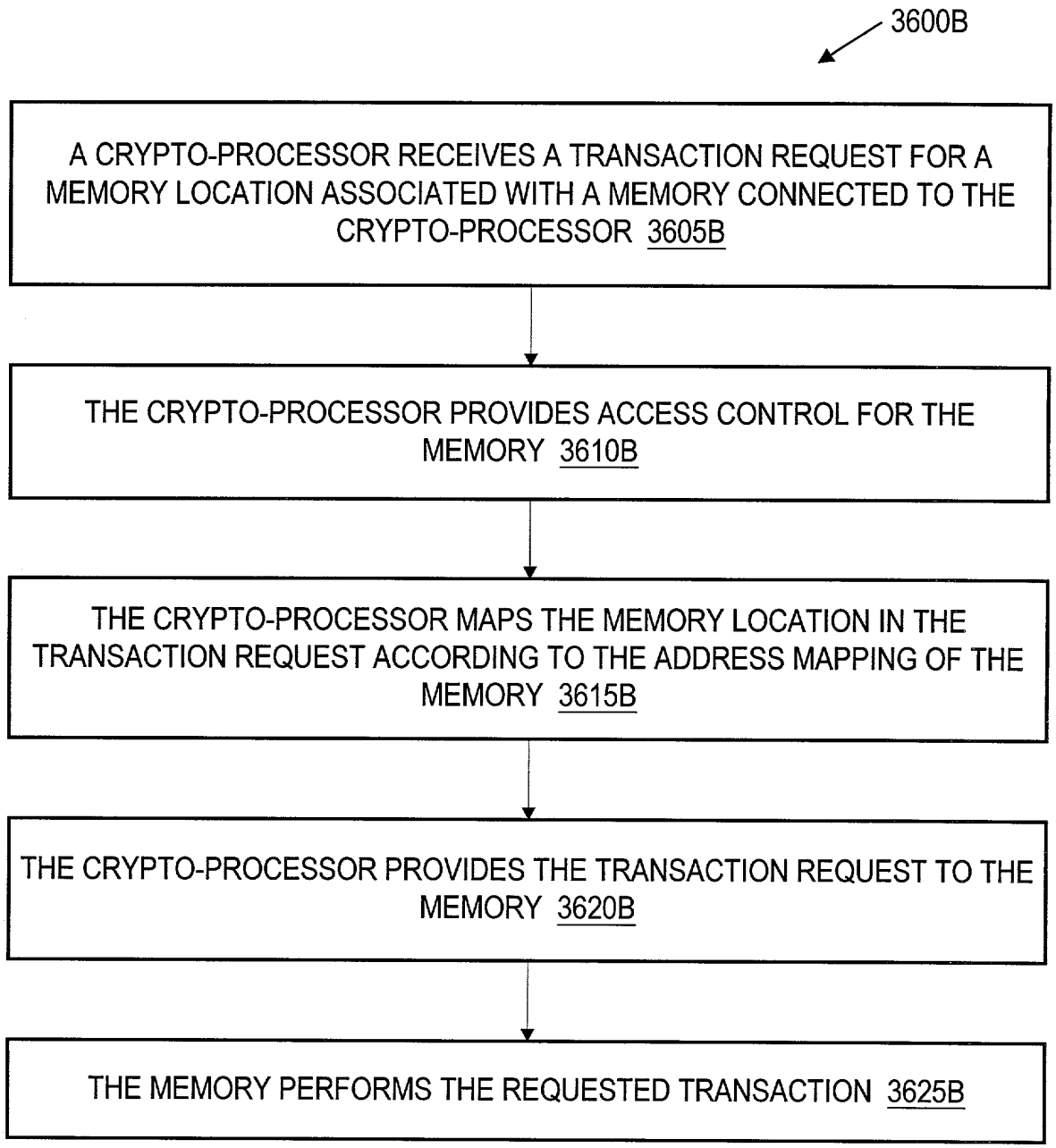

3600B
A CRYPTO-PROCESSOR RECEIVES A TRANSACTION REQUEST FOR A MEMORY LOCATION ASSOCIATED WITH A MEMORY CONNECTED TO THE CRYPTO-PROCESSOR 3605B
THE CRYPTO-PROCESSOR PROVIDES ACCESS CONTROL FOR THE MEMORY 3610B
THE CRYPTO-PROCESSOR MAPS THE MEMORY LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE MEMORY 3615B
THE CRYPTO-PROCESSOR PROVIDES THE TRANSACTION REQUEST TO THE MEMORY 3620B
THE MEMORY PERFORMS THE REQUESTED TRANSACTION 3625B

Fig. 25B

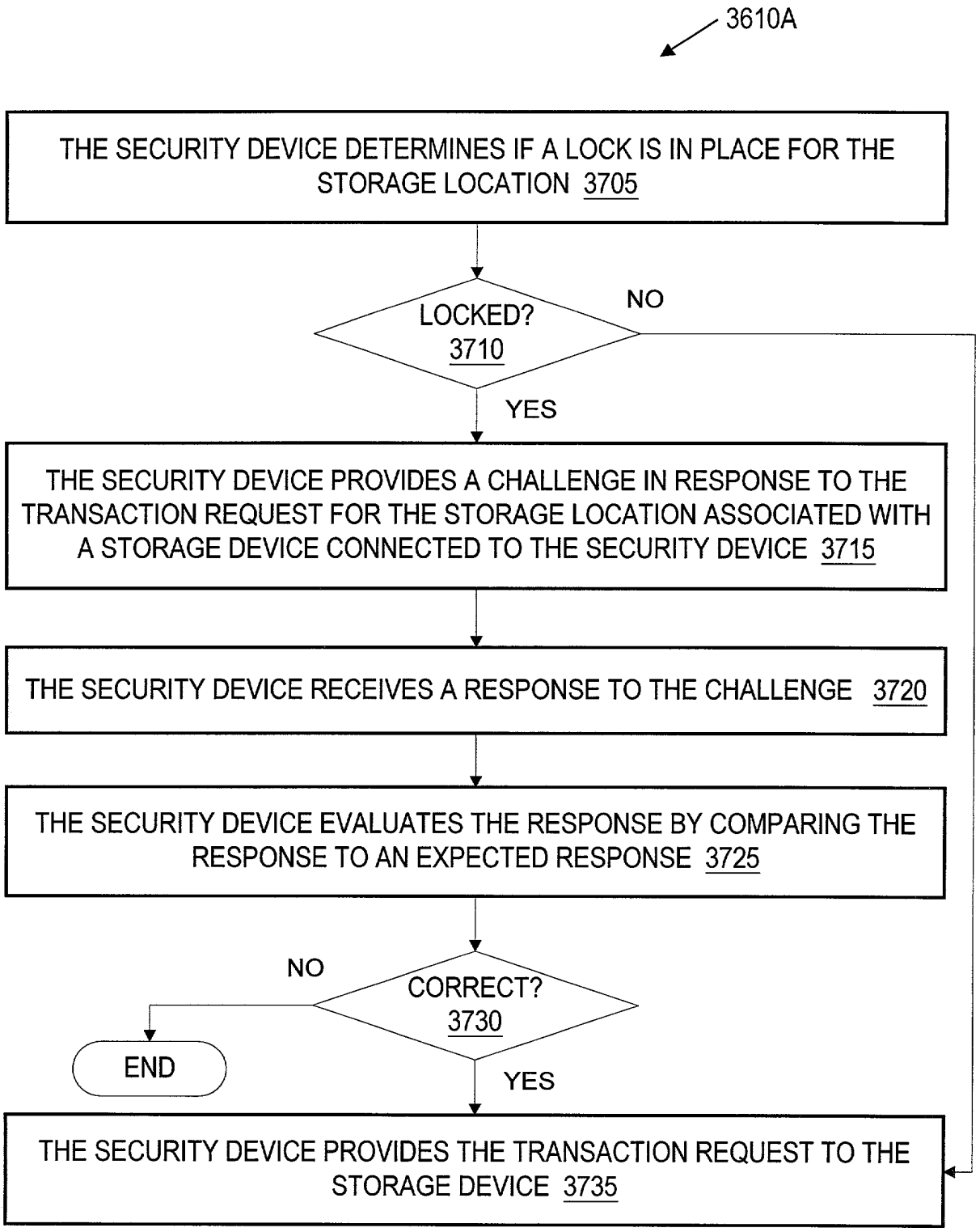

3610A
THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION 3705
LOCKED? 3710
NO
YES
THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3715
THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE 3720
THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE 3725
NO
CORRECT? 3730
END
YES
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3735

Fig. 26

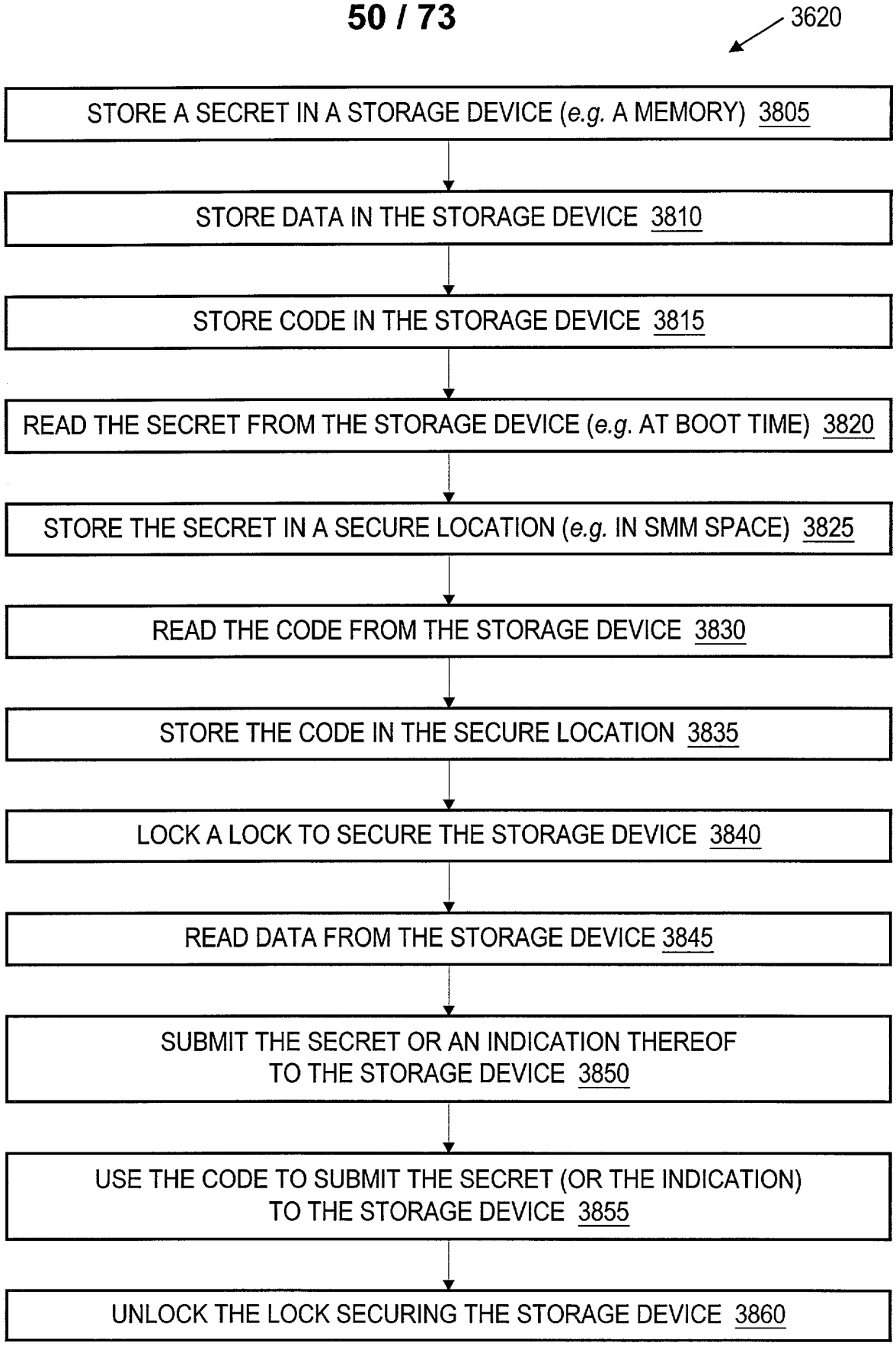
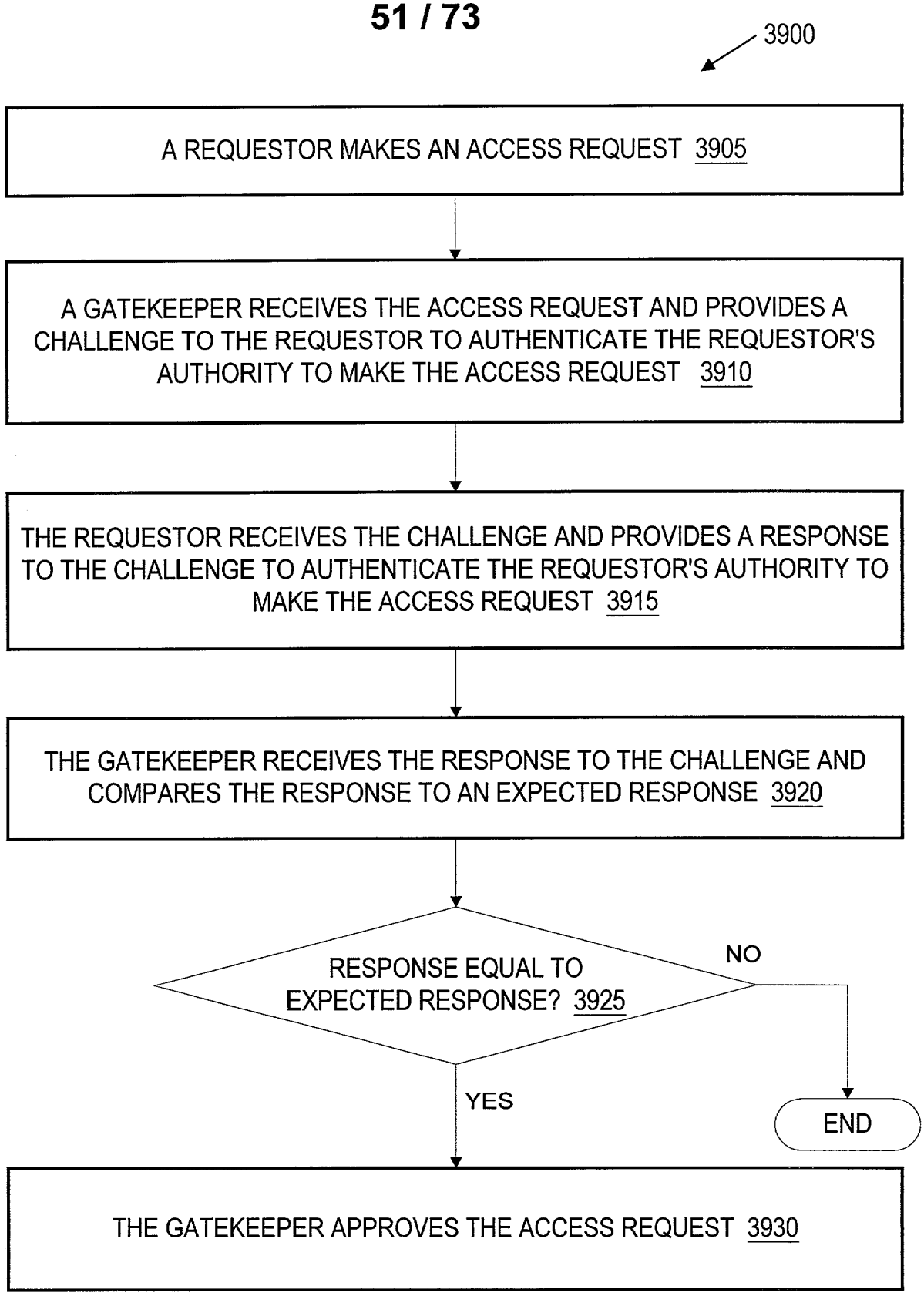


Fig. 27

Docket No. 50325-4001



T0065G0 +1801 /3650

Fig. 28
(Prior Art)

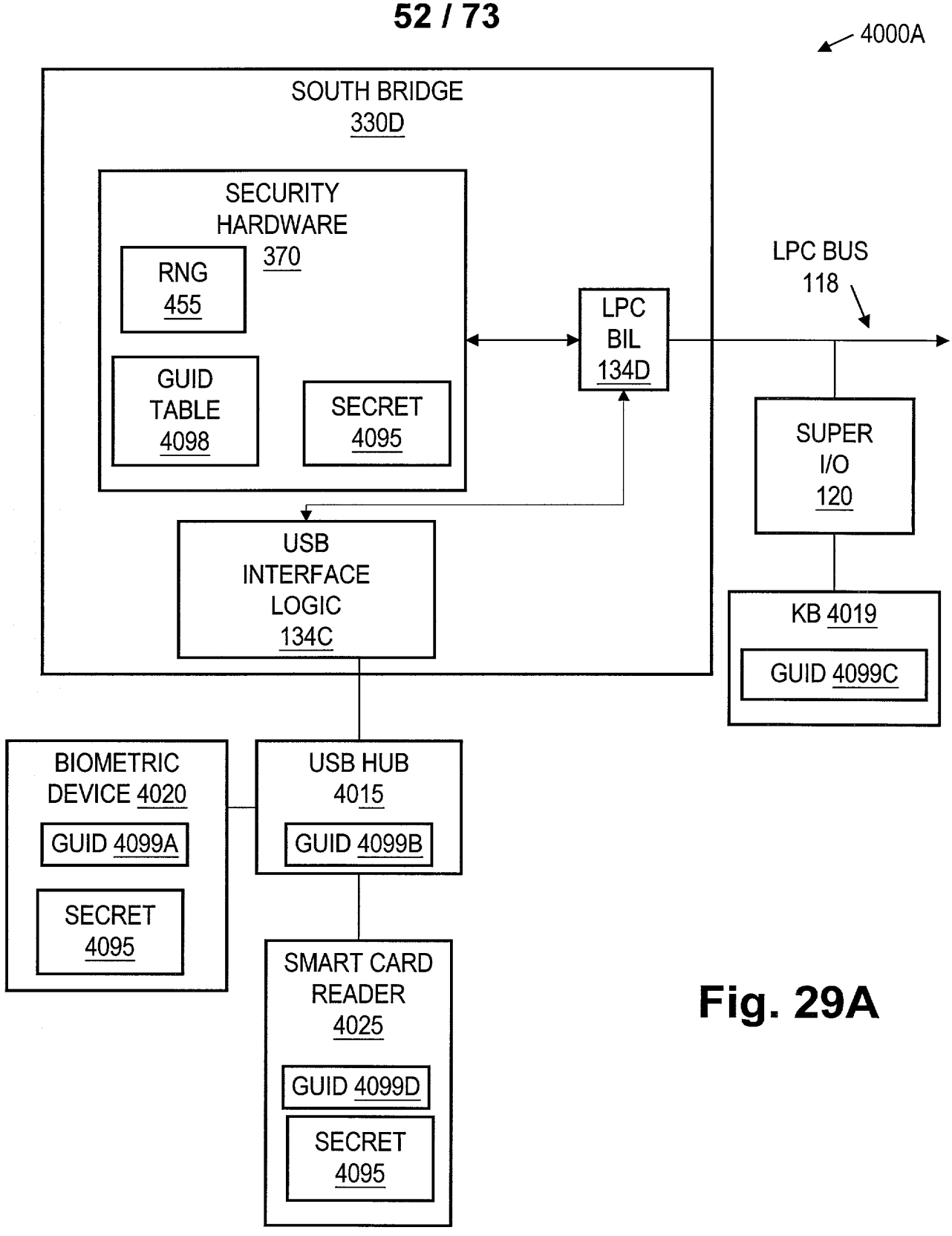


Fig. 29A

FD0550-1501/650

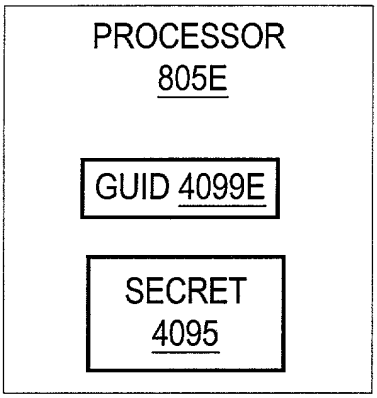


Fig. 29B

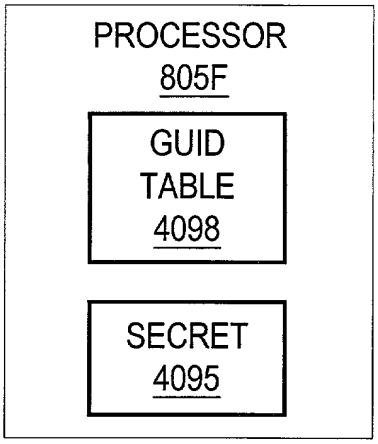


Fig. 29C

Express Mail Label No. EV339047050US

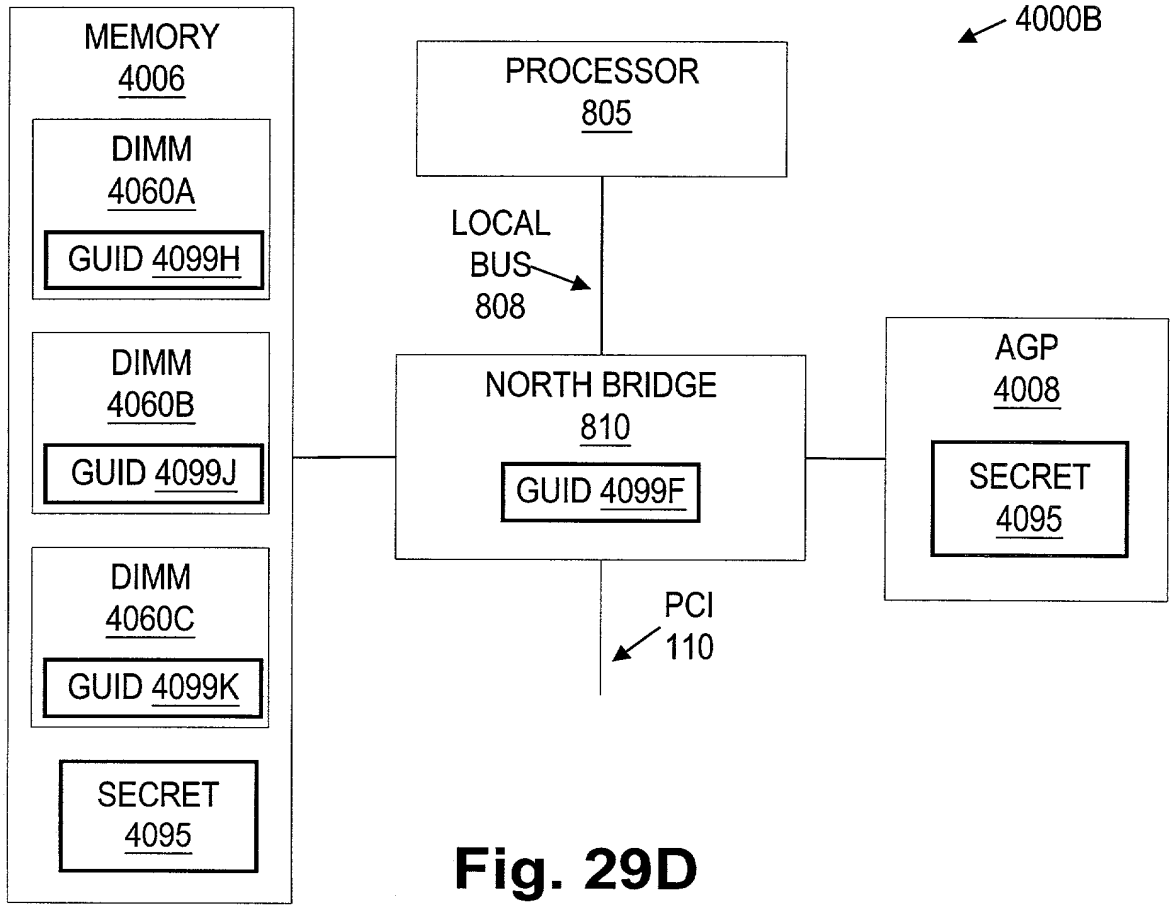


Fig. 29D

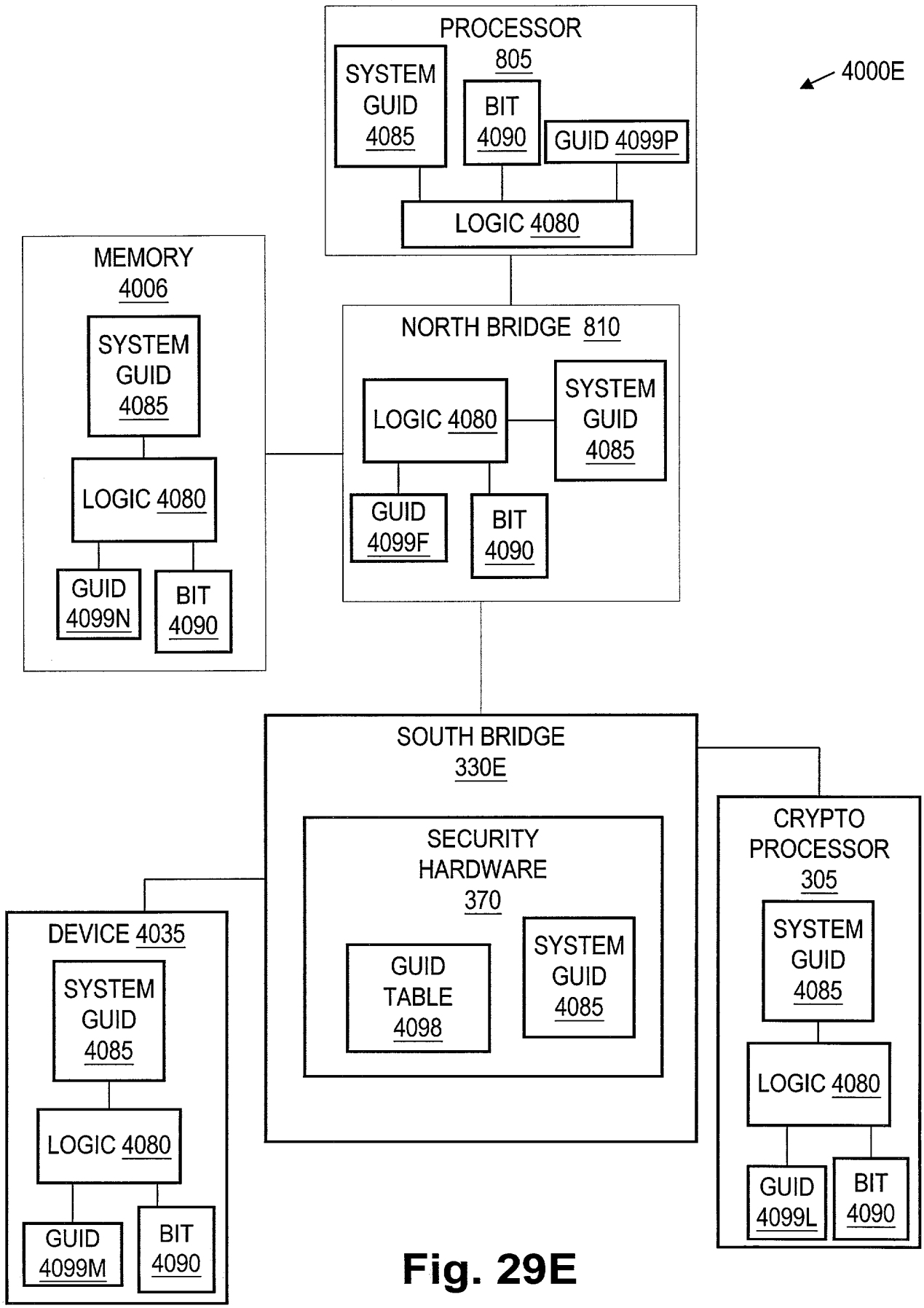


Fig. 29E

FOUNDATION-1807260

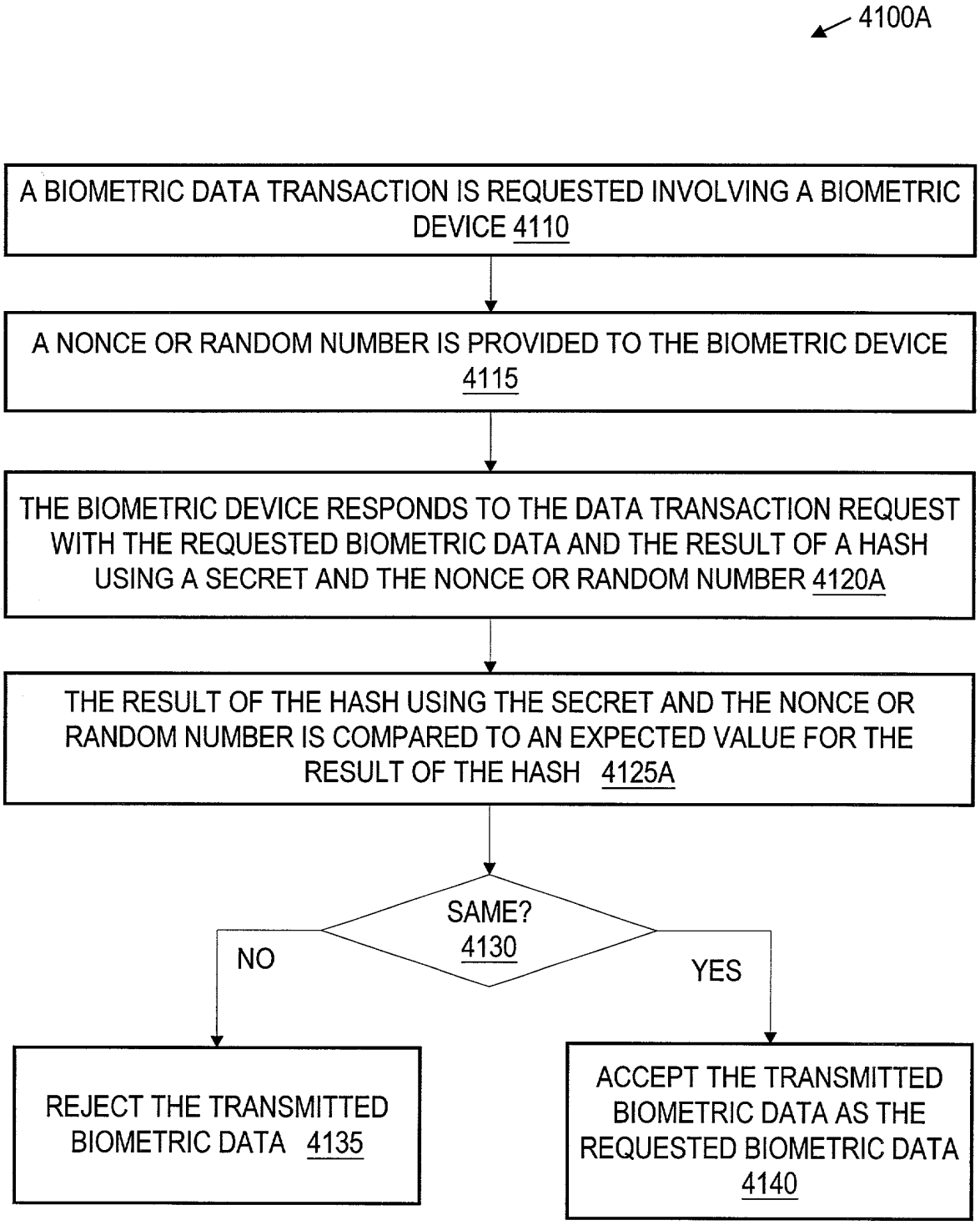

4100A
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125A
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30A

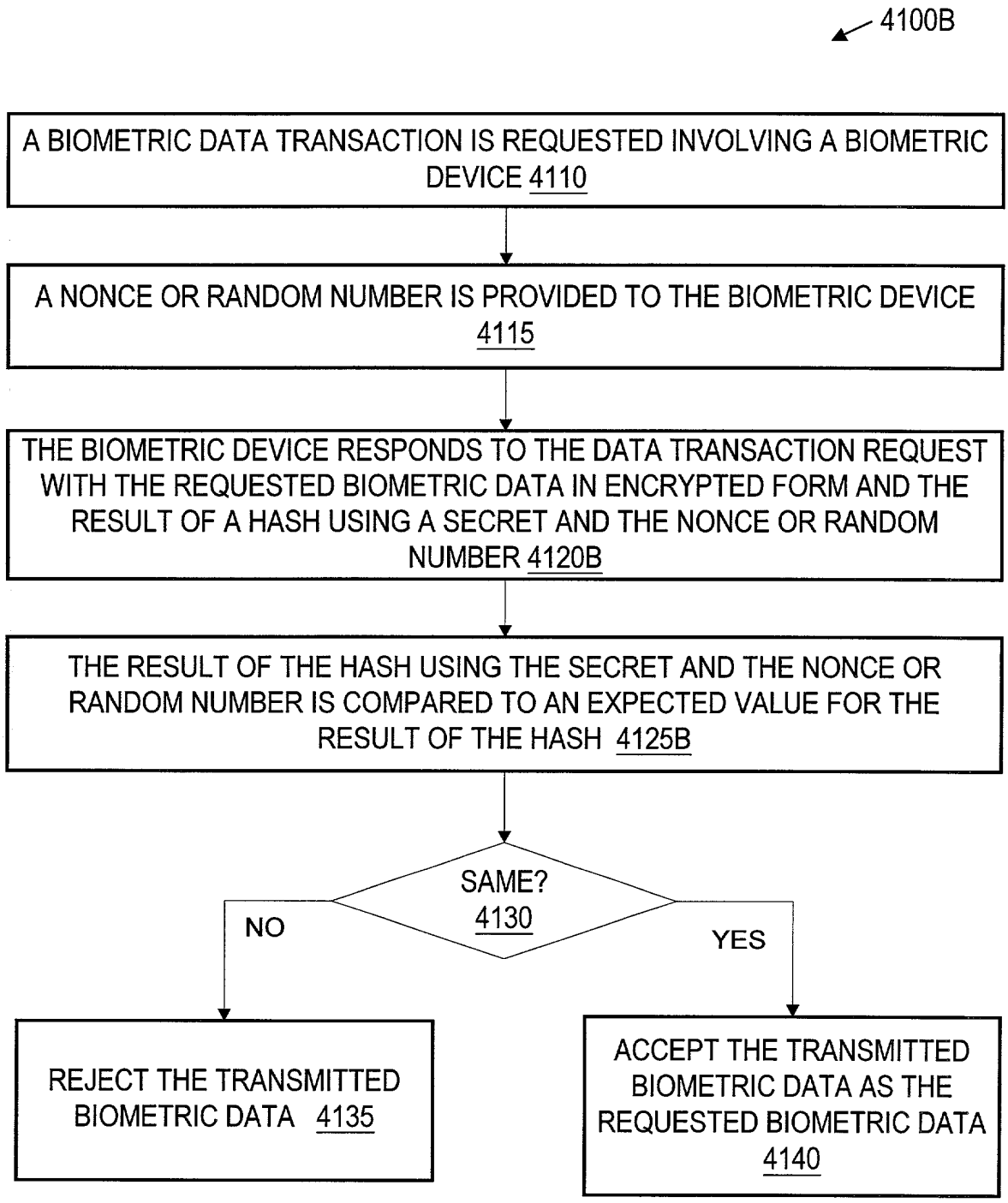

4100B
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA IN ENCRYPTED FORM AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120B
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125B
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30B

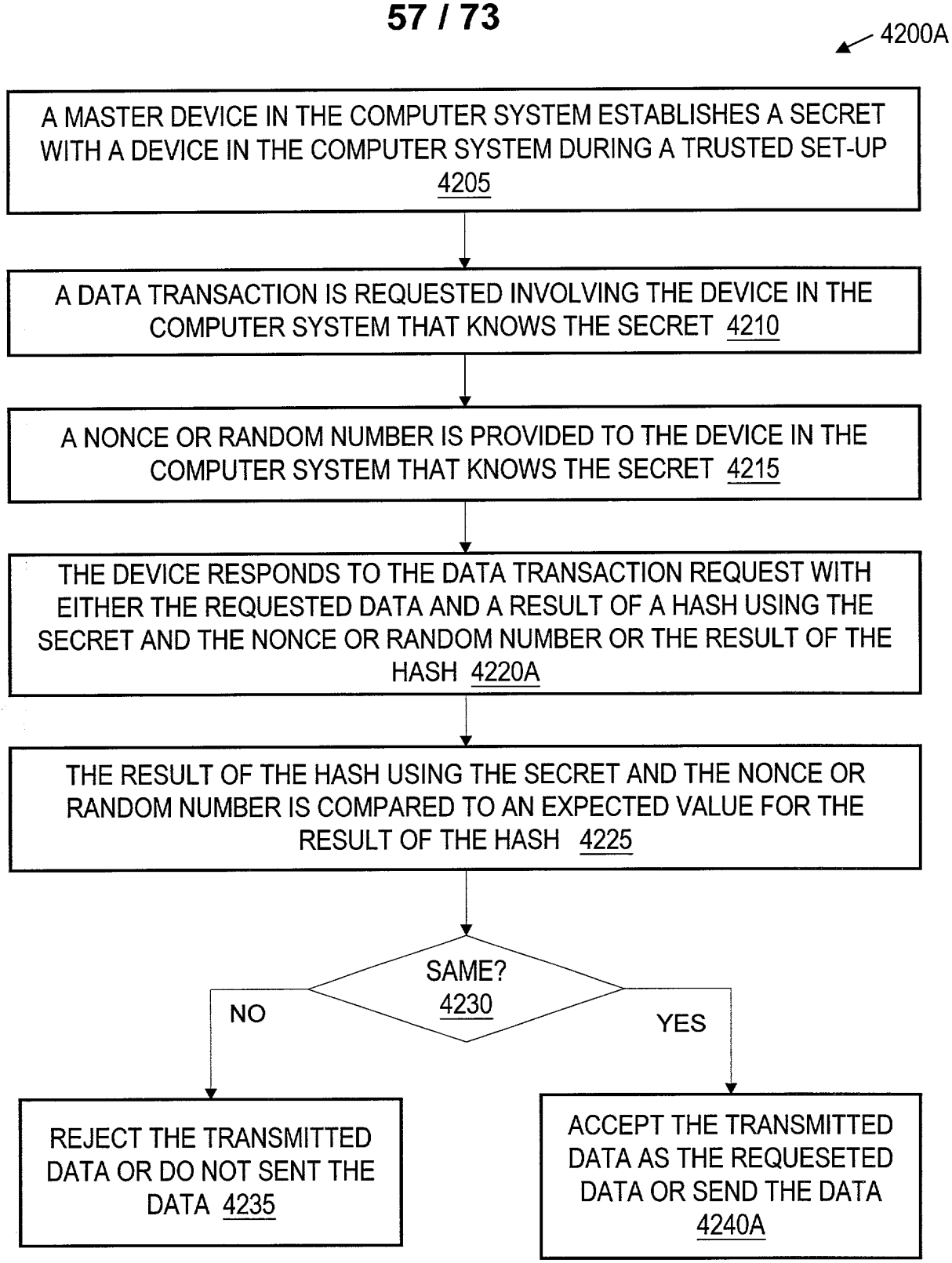

4200A
A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET WITH A DEVICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP 4205
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4210
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4215
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH EITHER THE REQUESTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4220A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4225
SAME? 4230
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4235
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA 4240A

Fig. 31A

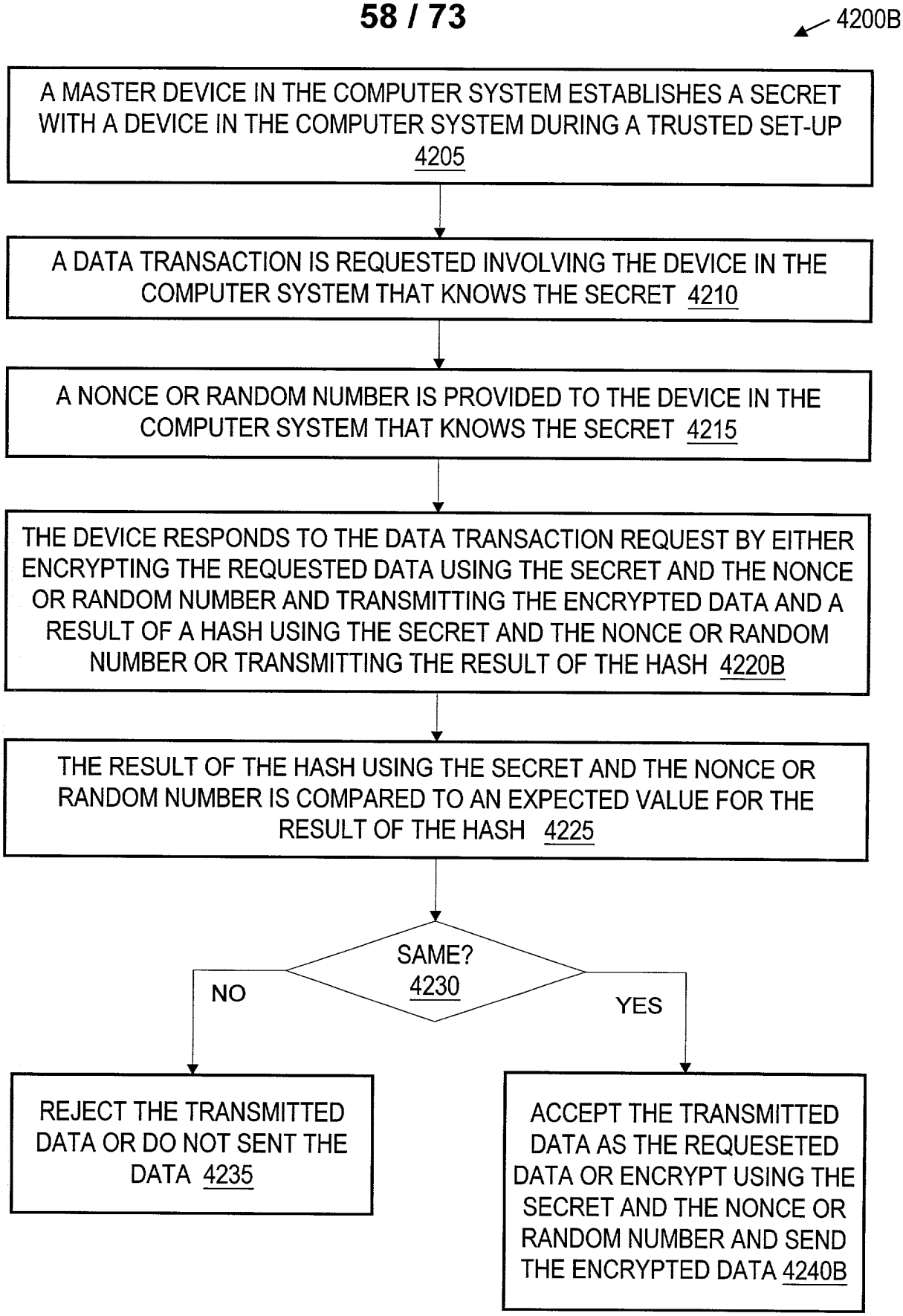
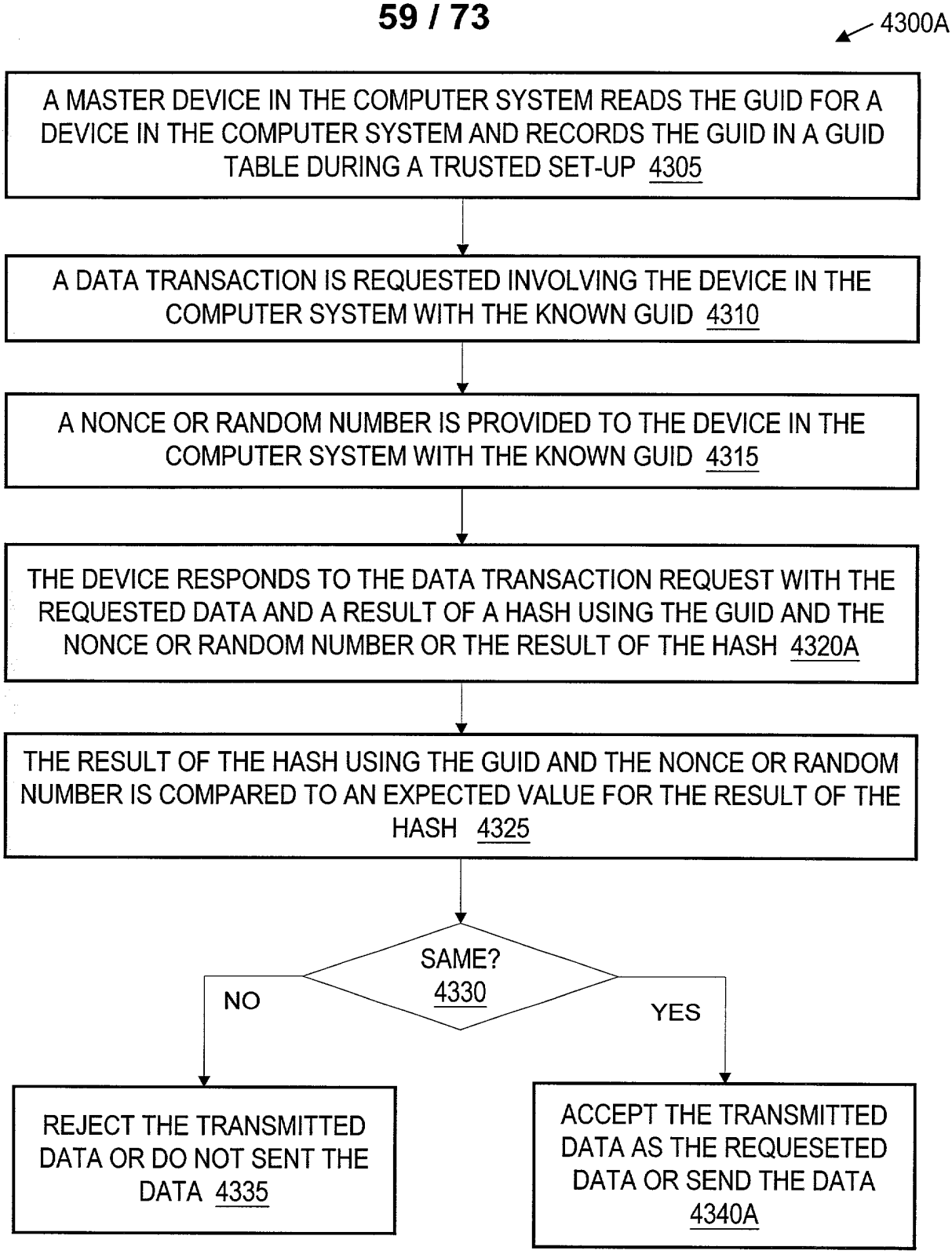


Fig. 31B

T-005250-4801-7960



T0025.P801/2660

Fig. 32A

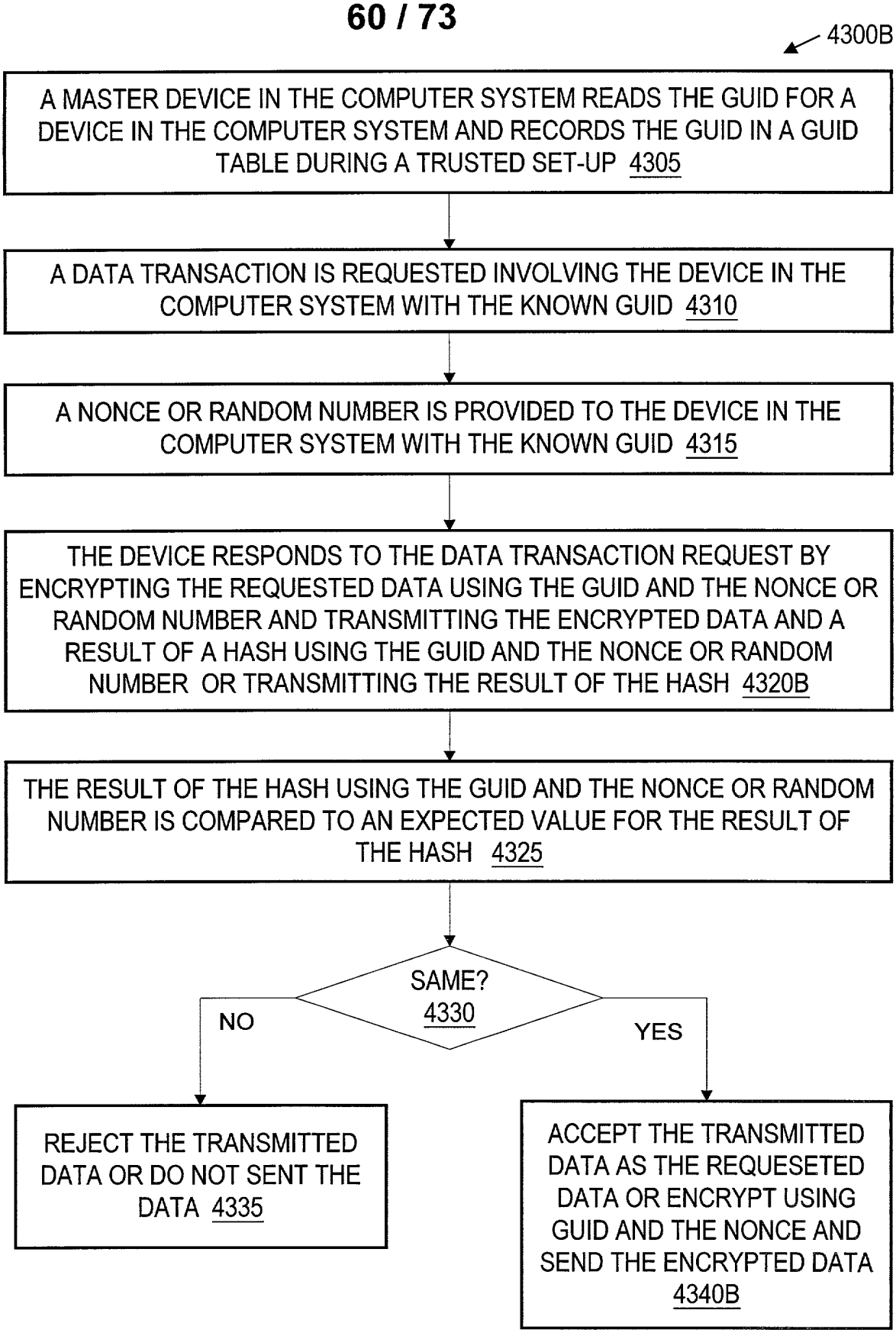


Fig. 32B

FOSS-4807369

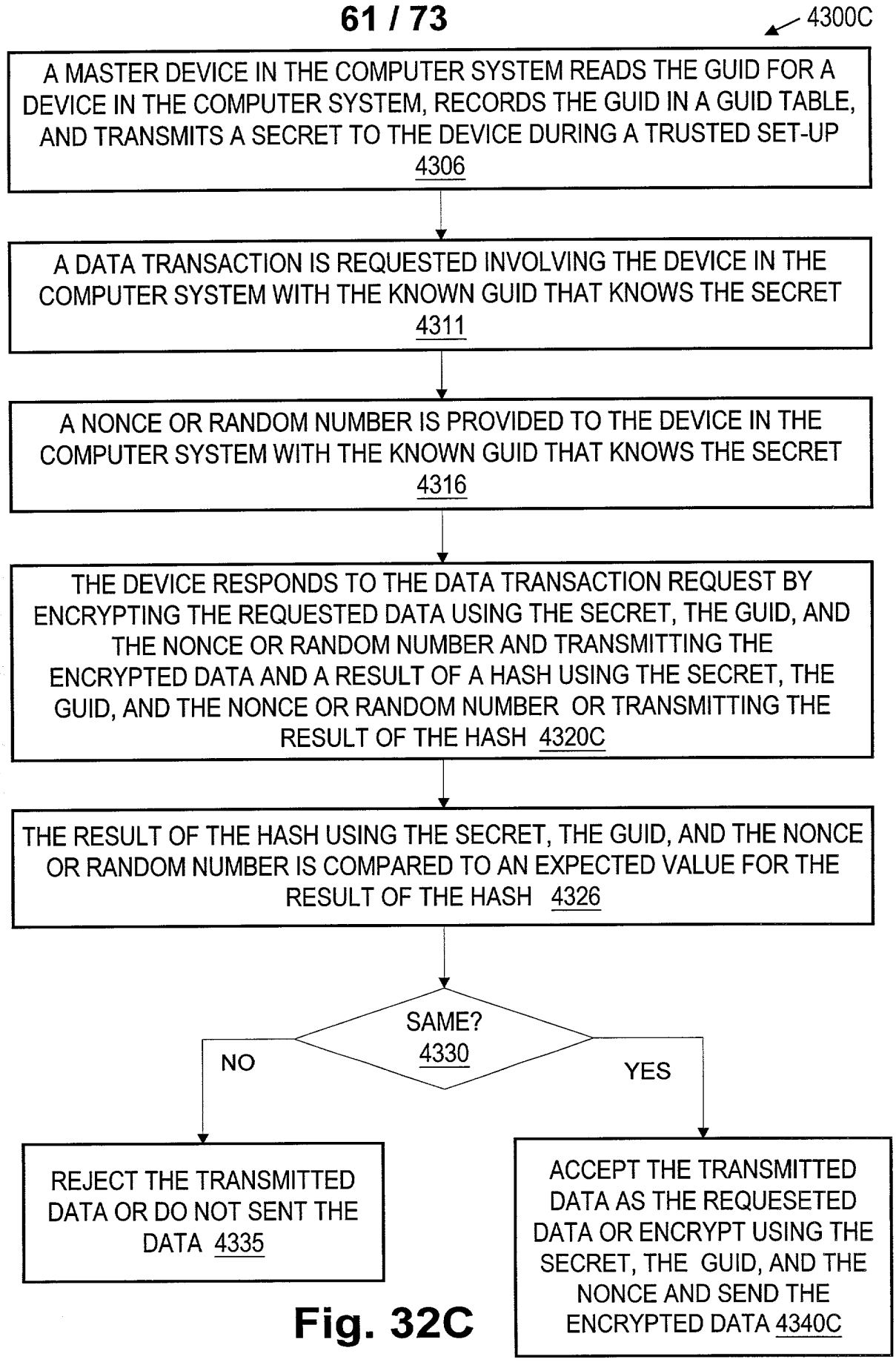


Fig. 32C

TT03763-US-PCT-3650

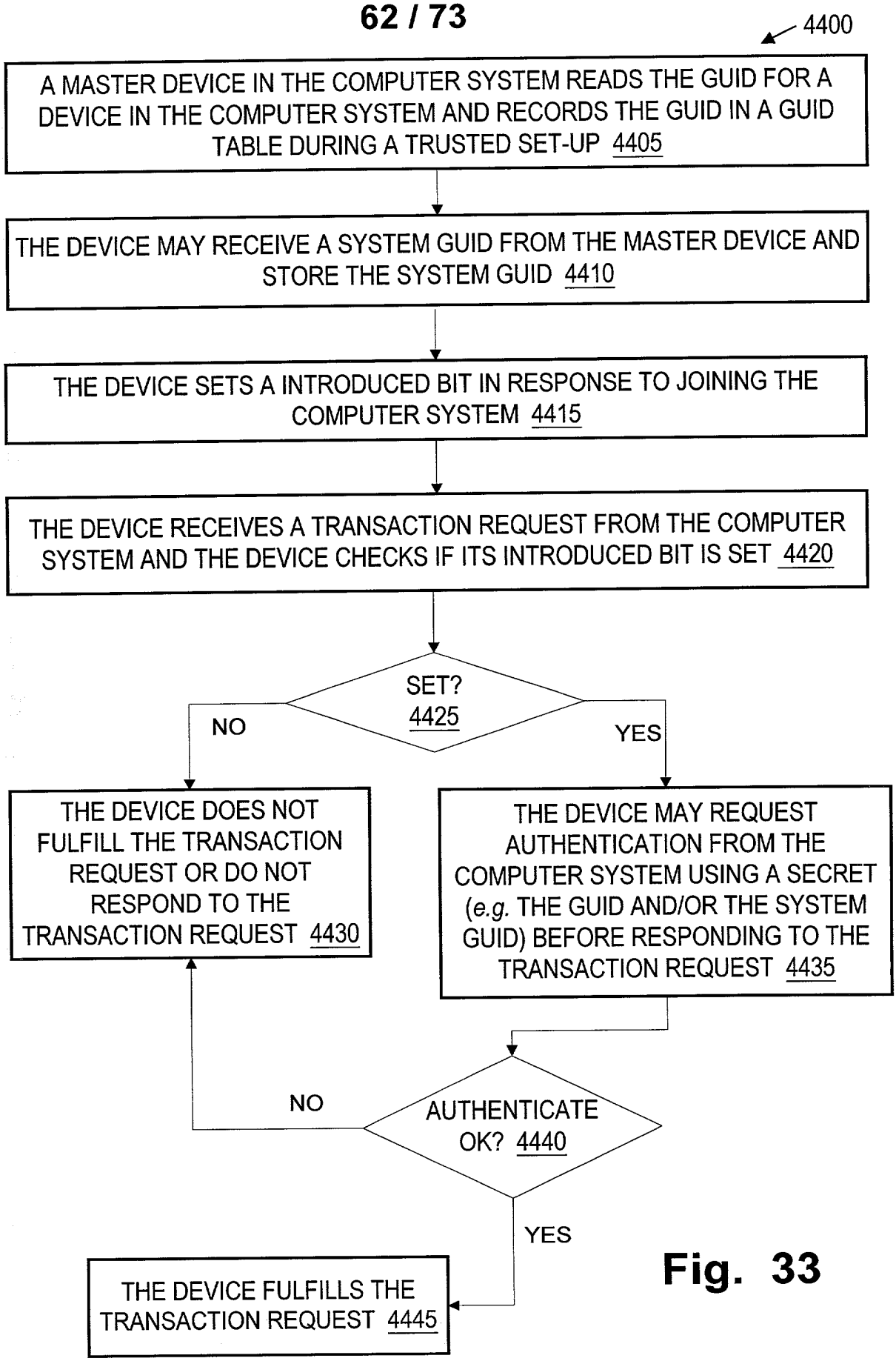

4400
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4405
THE DEVICE MAY RECEIVE A SYSTEM GUID FROM THE MASTER DEVICE AND STORE THE SYSTEM GUID 4410
THE DEVICE SETS A INTRODUCED BIT IN RESPONSE TO JOINING THE COMPUTER SYSTEM 4415
THE DEVICE RECEIVES A TRANSACTION REQUEST FROM THE COMPUTER SYSTEM AND THE DEVICE CHECKS IF ITS INTRODUCED BIT IS SET 4420
SET? 4425
NO
YES
THE DEVICE DOES NOT FULFILL THE TRANSACTION REQUEST OR DO NOT RESPOND TO THE TRANSACTION REQUEST 4430
THE DEVICE MAY REQUEST AUTHENTICATION FROM THE COMPUTER SYSTEM USING A SECRET (e.g. THE GUID AND/OR THE SYSTEM GUID) BEFORE RESPONDING TO THE TRANSACTION REQUEST 4435
NO
AUTHENTICATE OK? 4440
YES
THE DEVICE FULFILLS THE TRANSACTION REQUEST 4445

Fig. 33

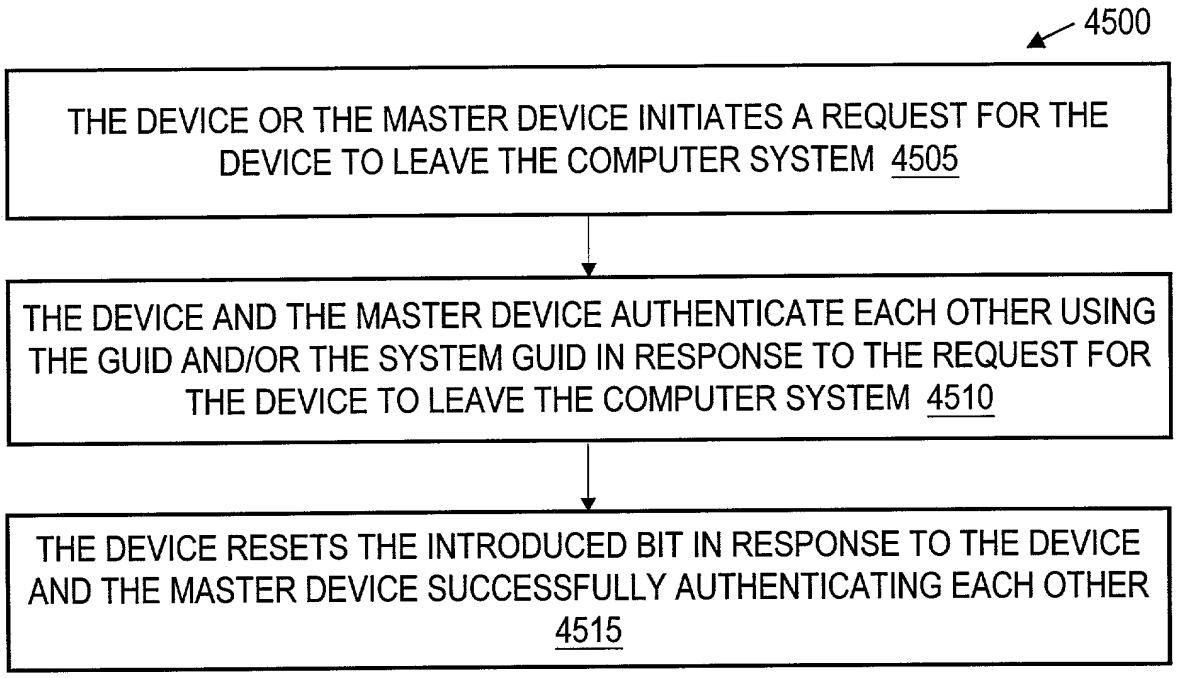


Fig. 34

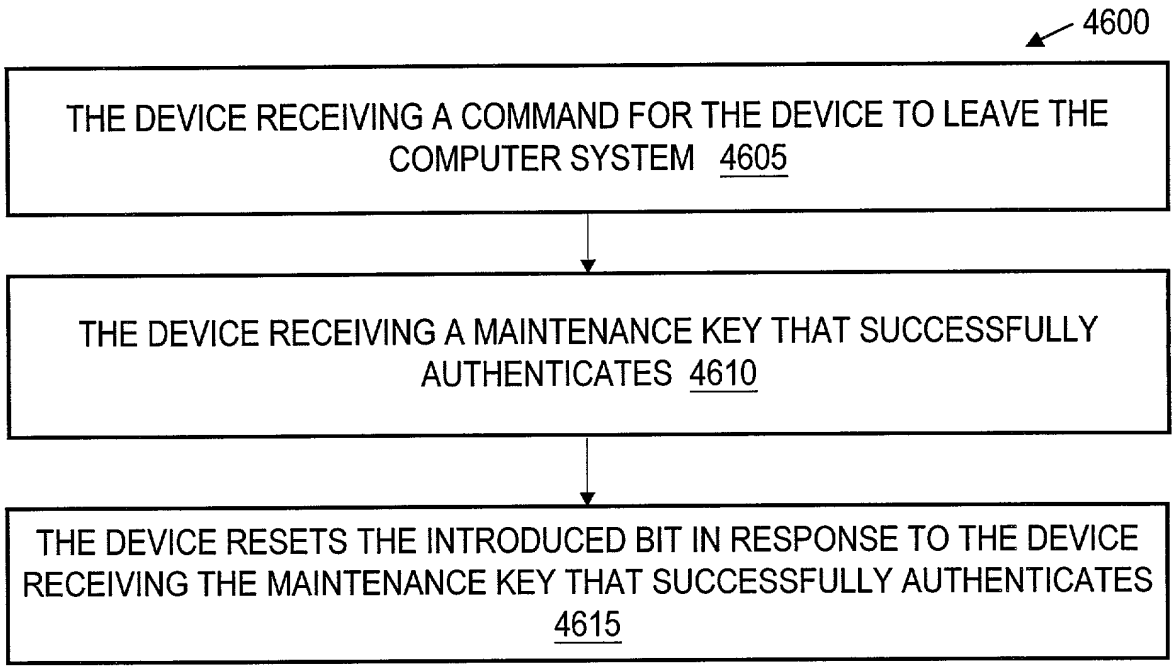


Fig. 35

Doc. 4 of 5 - 2007-10-04

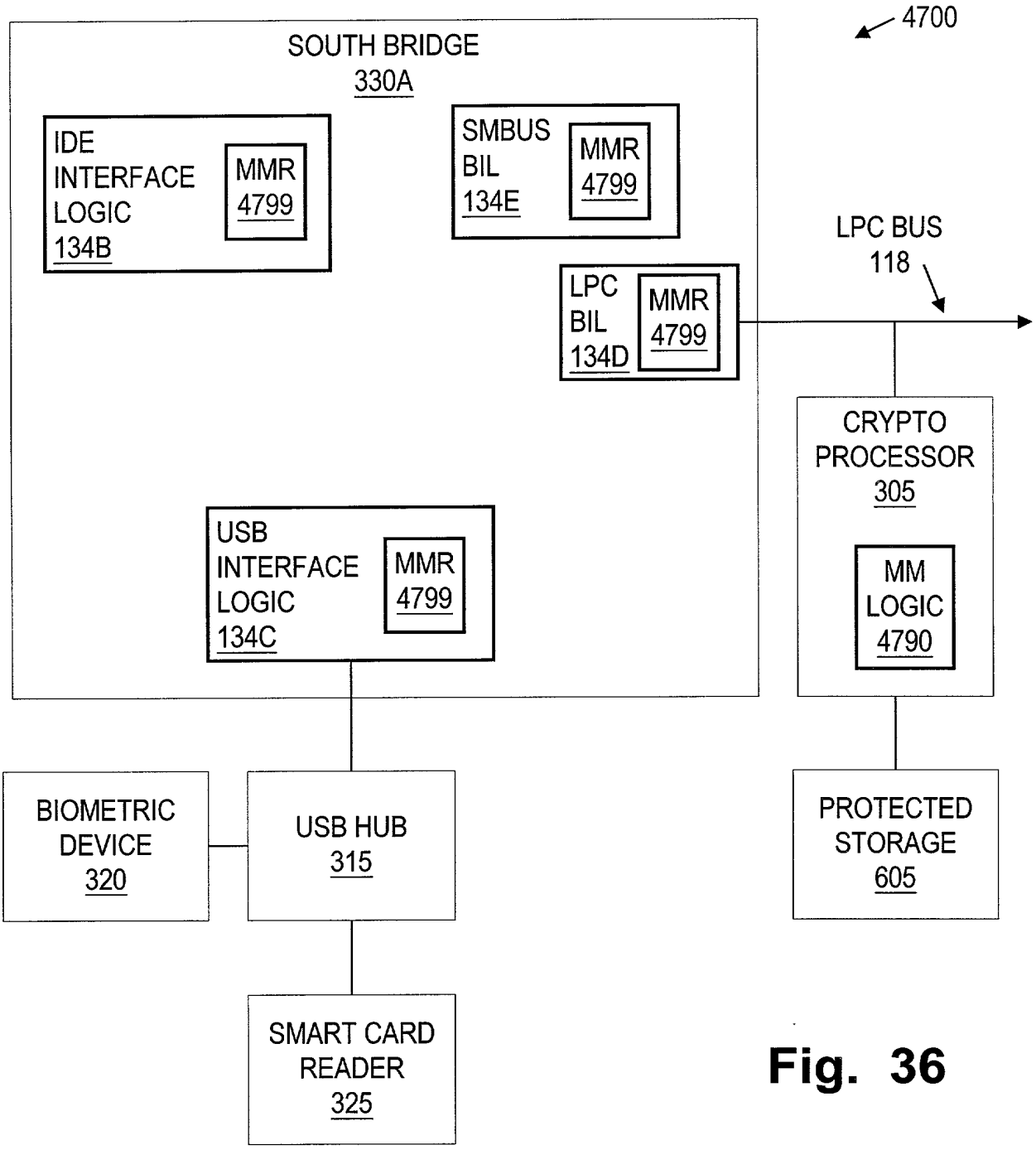
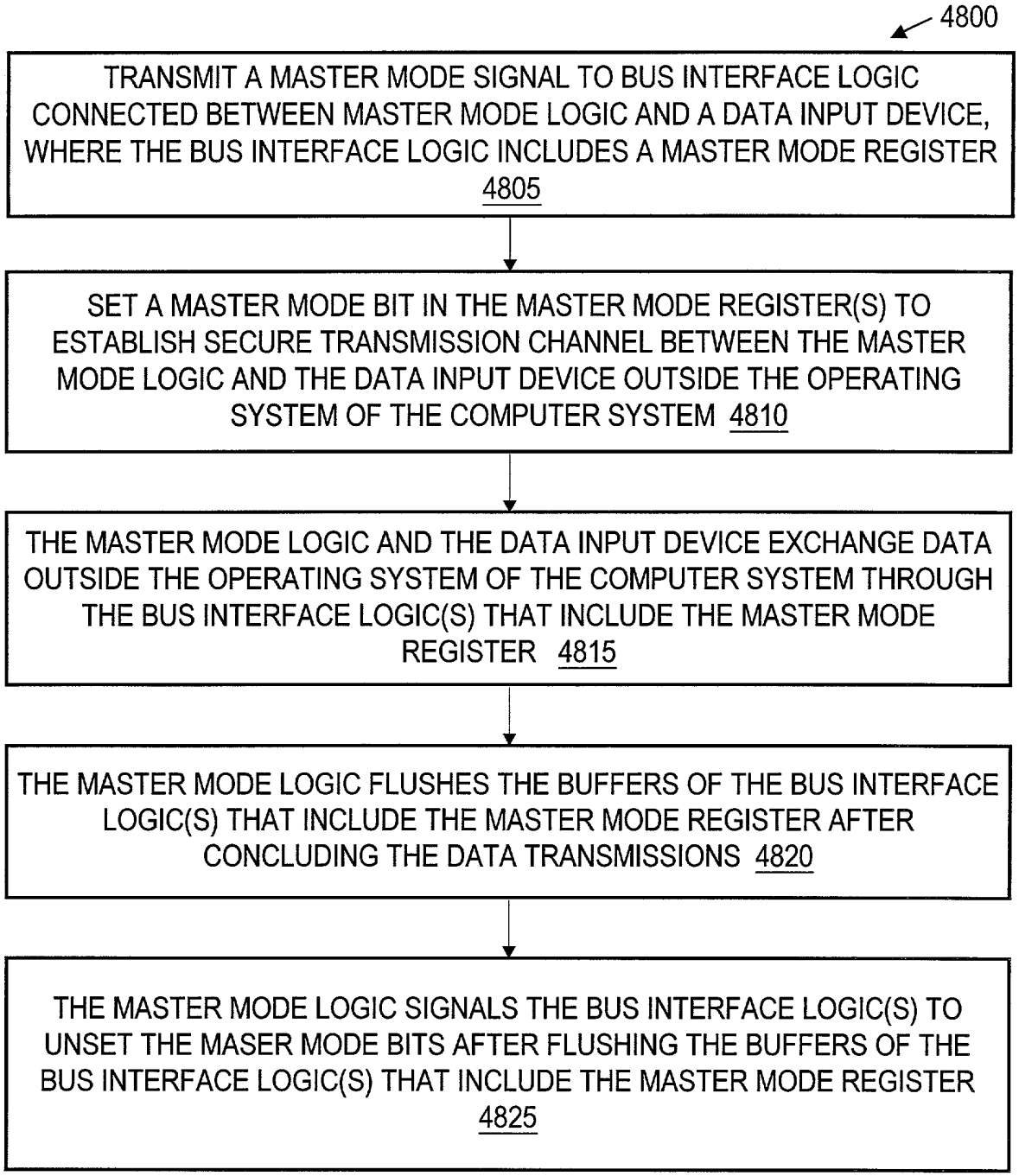


Fig. 36

FOUNDATION-1007



TT03750 +1807/650

Fig. 37

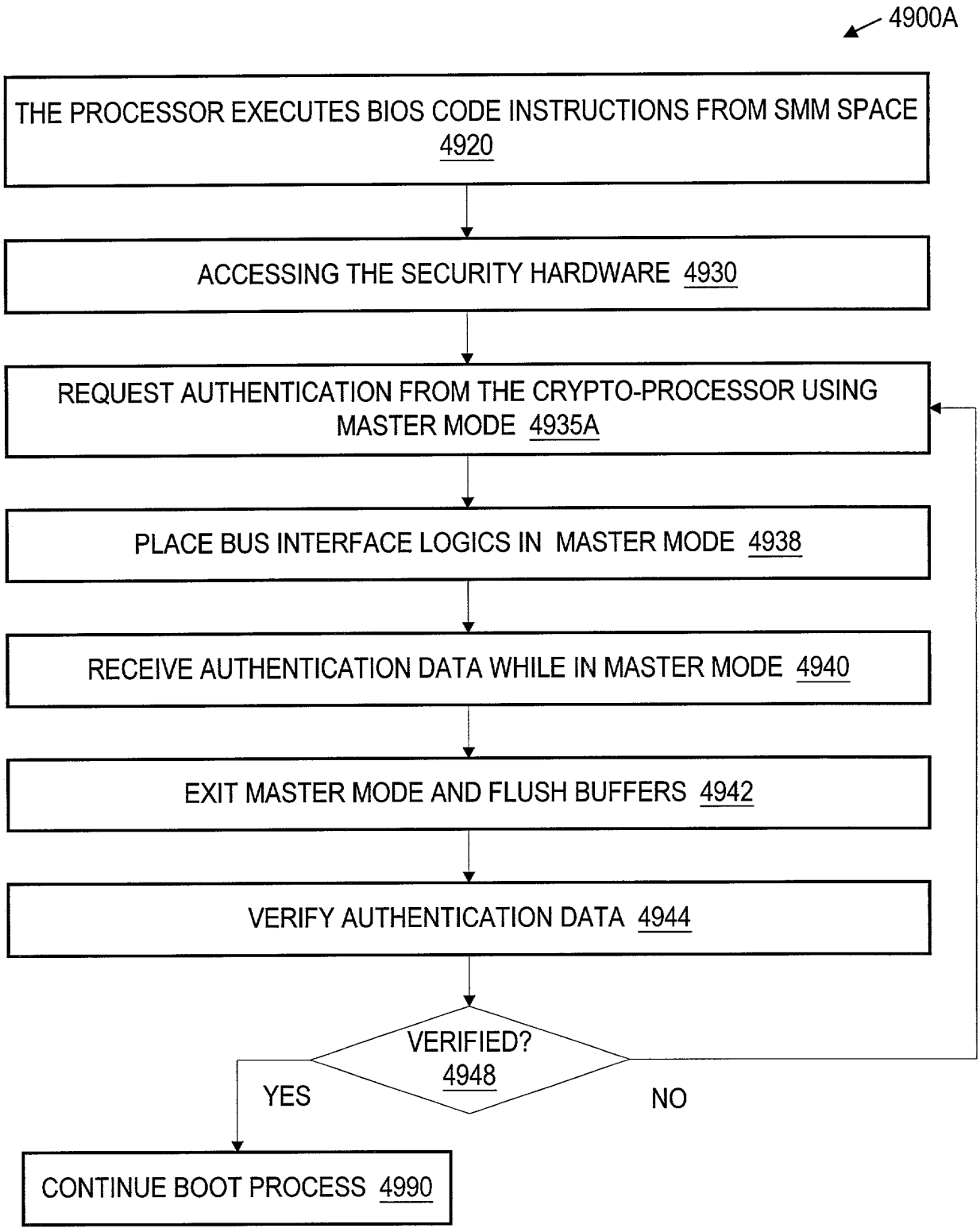

4900A
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
REQUEST AUTHENTICATION FROM THE CRYPTO-PROCESSOR USING MASTER MODE 4935A
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38A

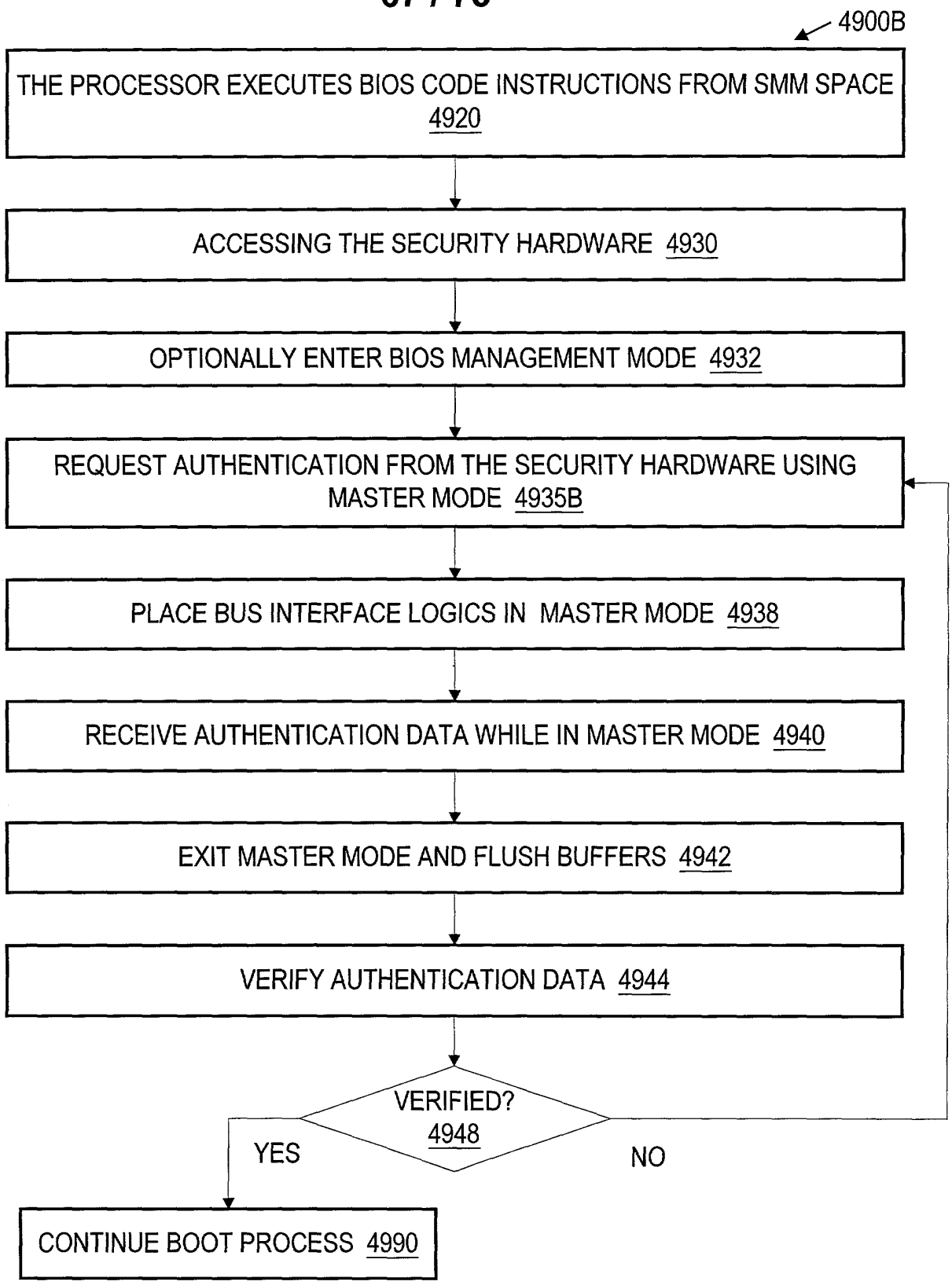

4900B
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
OPTIONALLY ENTER BIOS MANAGEMENT MODE 4932
REQUEST AUTHENTICATION FROM THE SECURITY HARDWARE USING MASTER MODE 4935B
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38B

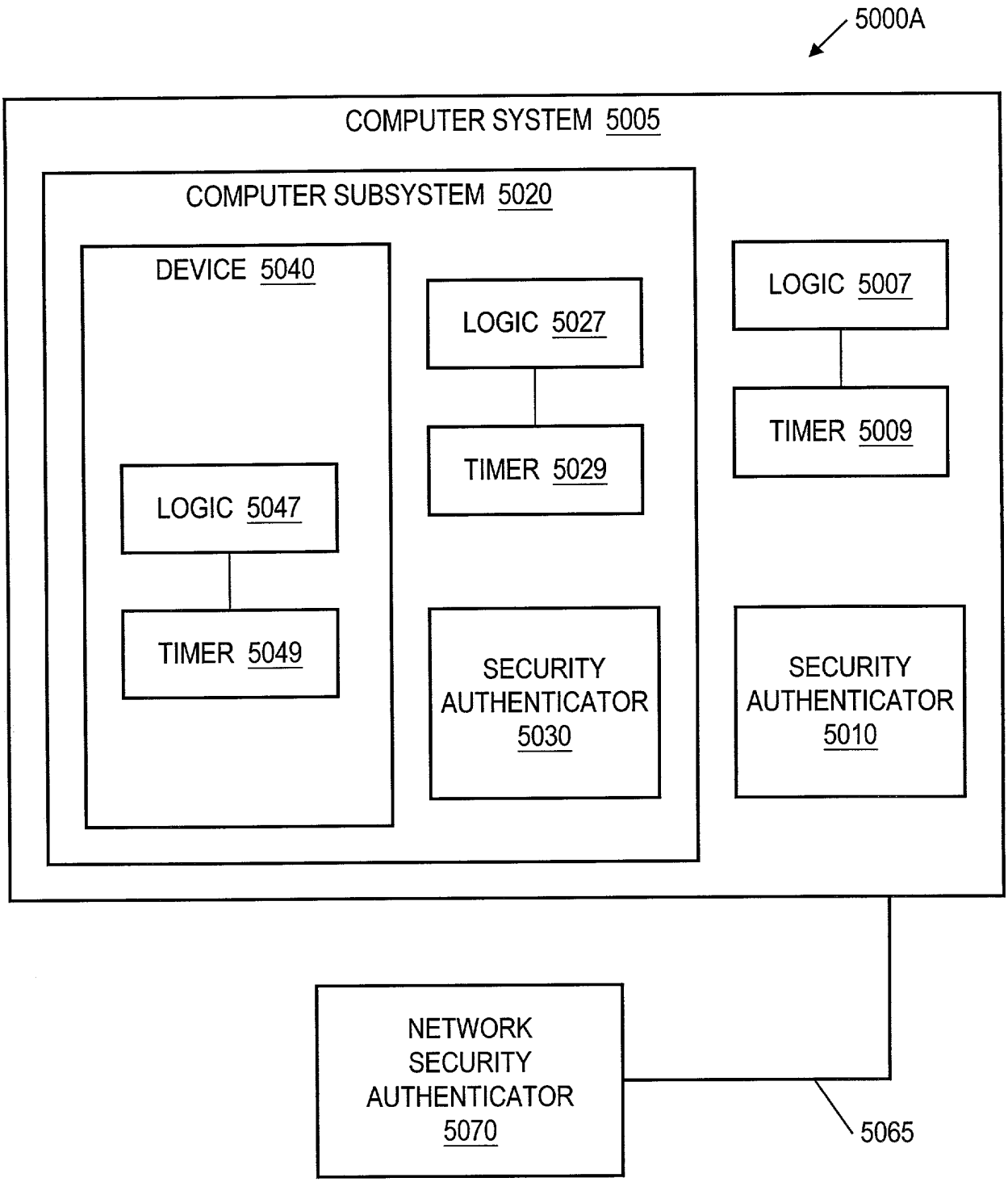

5000A
COMPUTER SYSTEM 5005
COMPUTER SUBSYSTEM 5020
DEVICE 5040
LOGIC 5047
TIMER 5049
LOGIC 5027
TIMER 5029
SECURITY AUTHENTICATOR 5030
LOGIC 5007
TIMER 5009
SECURITY AUTHENTICATOR 5010
NETWORK SECURITY AUTHENTICATOR 5070
5065

Fig. 39A

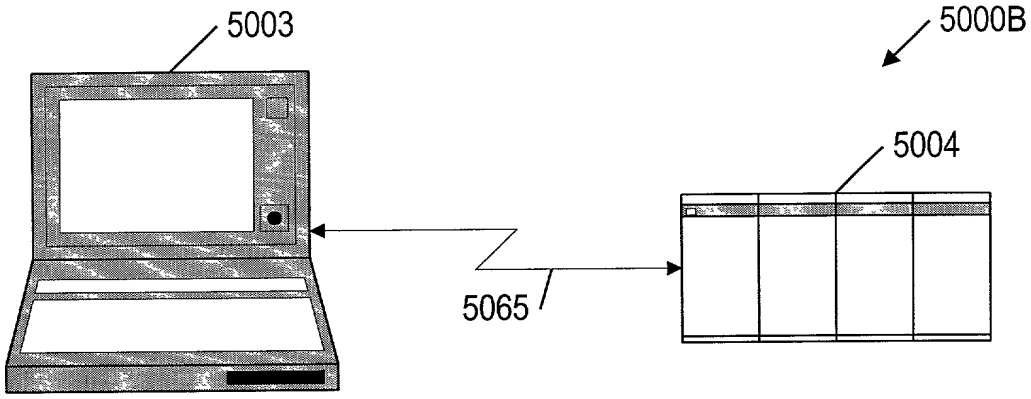


Fig. 39B

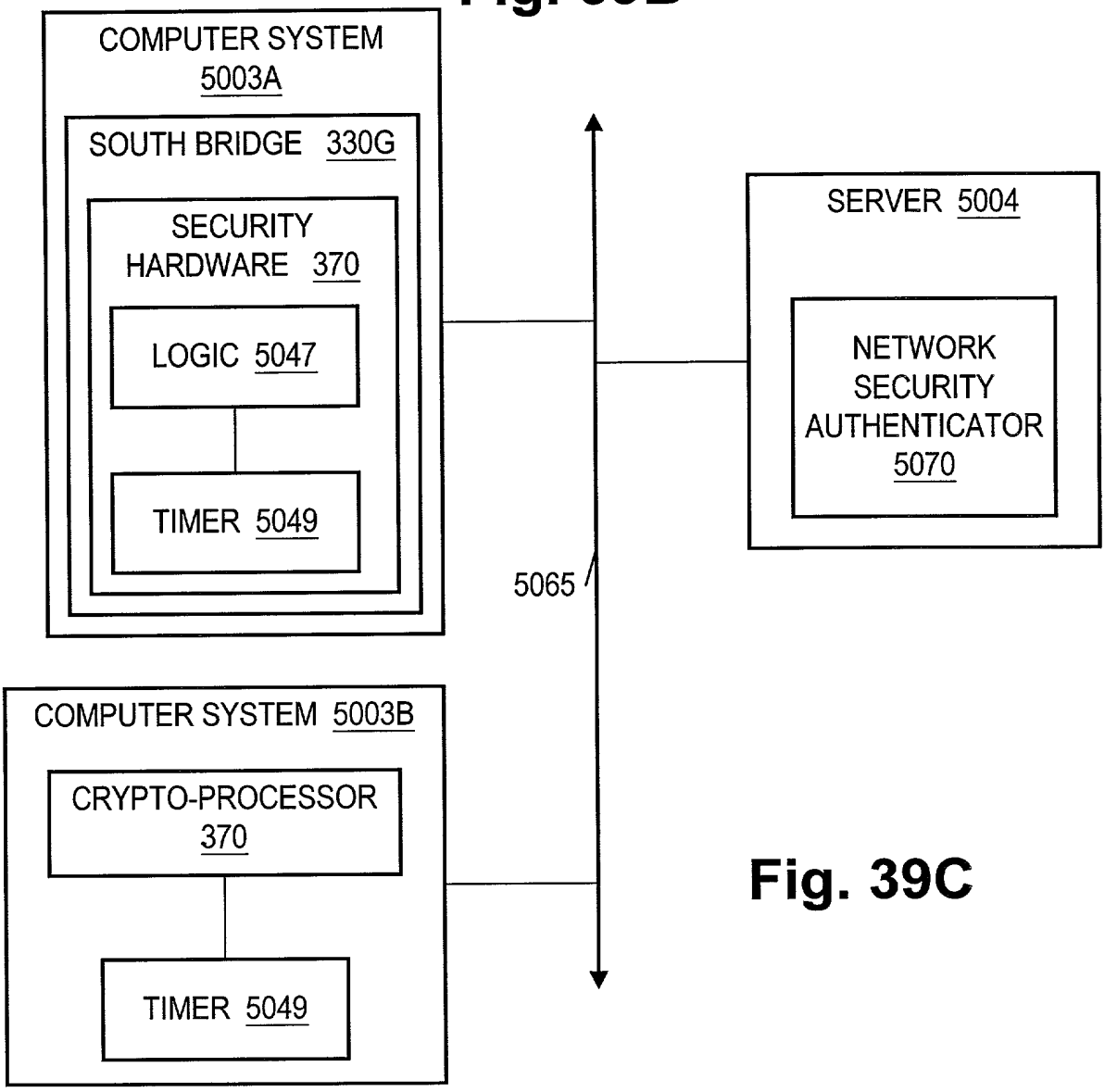


Fig. 39C

TT0563-1601-7650

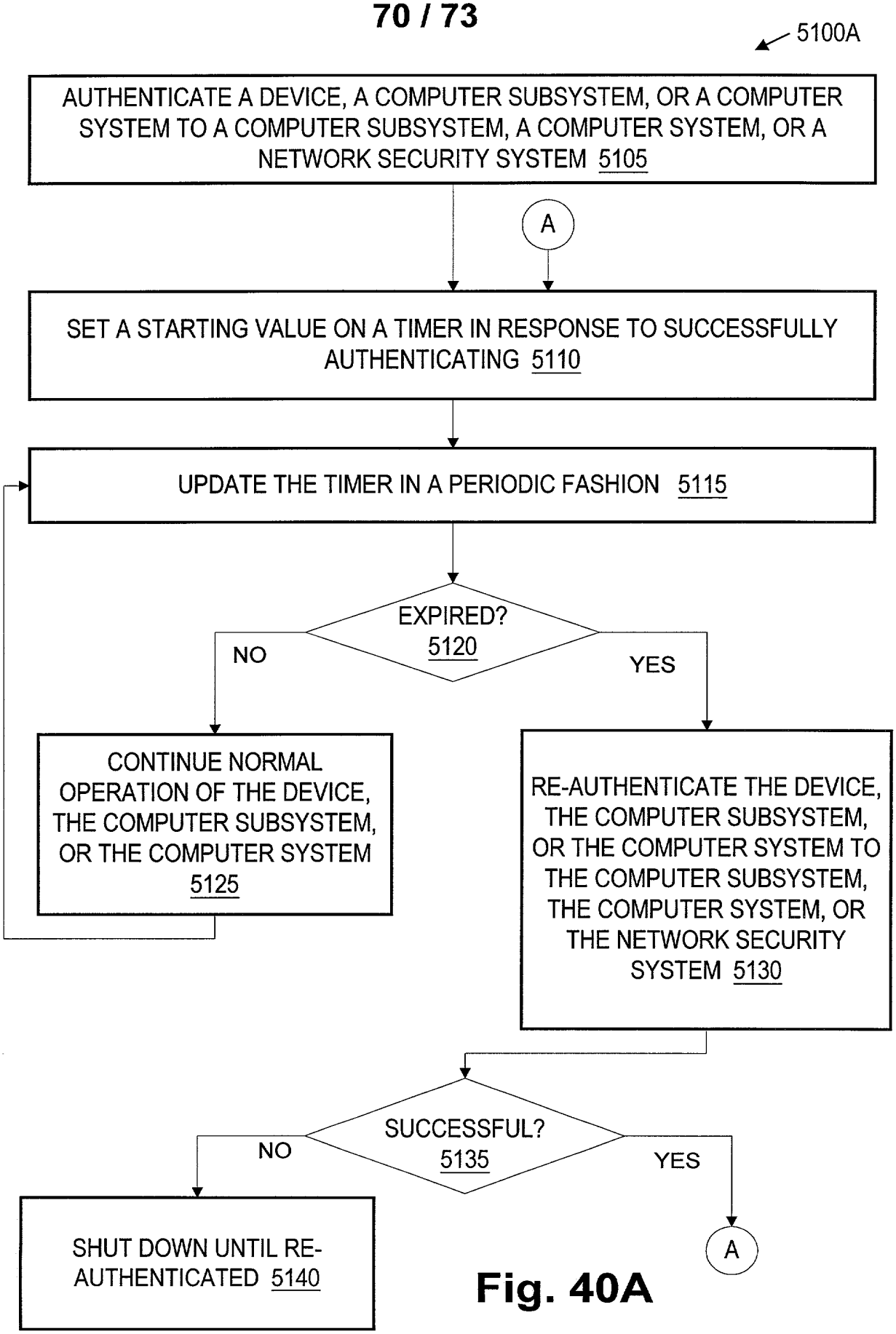


Fig. 40A

TOSHIBA-1007

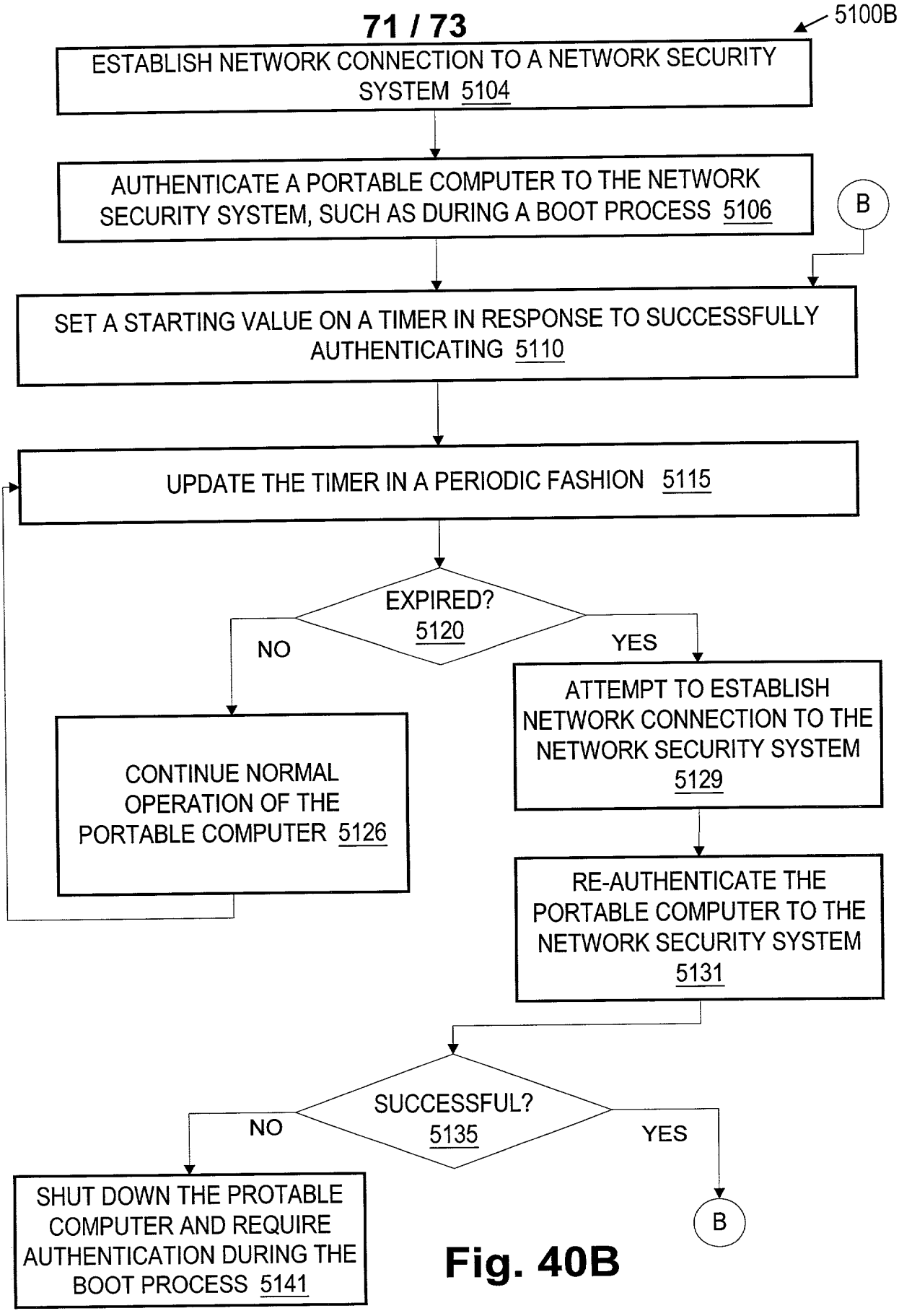


Fig. 40B

TT03763-1001F7350

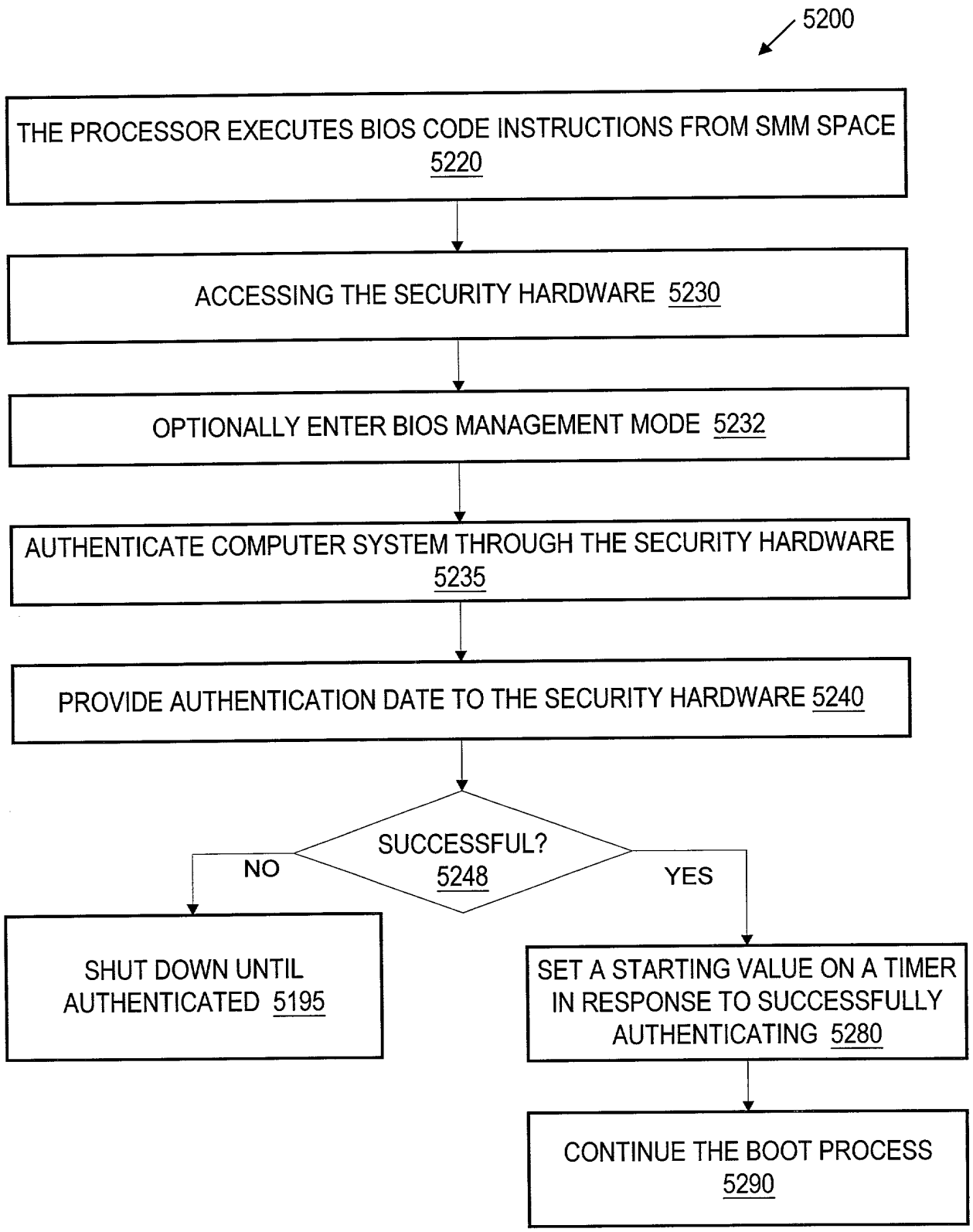

5200
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 5220
ACCESSING THE SECURITY HARDWARE 5230
OPTIONALLY ENTER BIOS MANAGEMENT MODE 5232
AUTHENTICATE COMPUTER SYSTEM THROUGH THE SECURITY HARDWARE 5235
PROVIDE AUTHENTICATION DATE TO THE SECURITY HARDWARE 5240
SUCCESSFUL? 5248
NO
YES
SHUT DOWN UNTIL AUTHENTICATED 5195
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING 5280
CONTINUE THE BOOT PROCESS 5290

Fig. 41

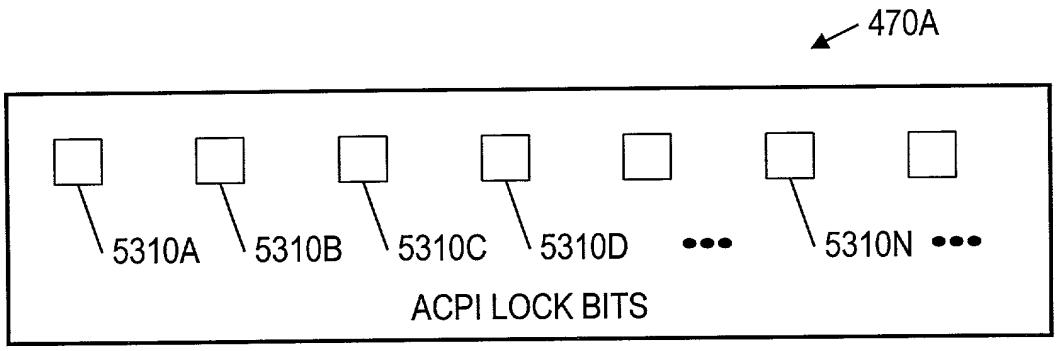


Fig. 42A

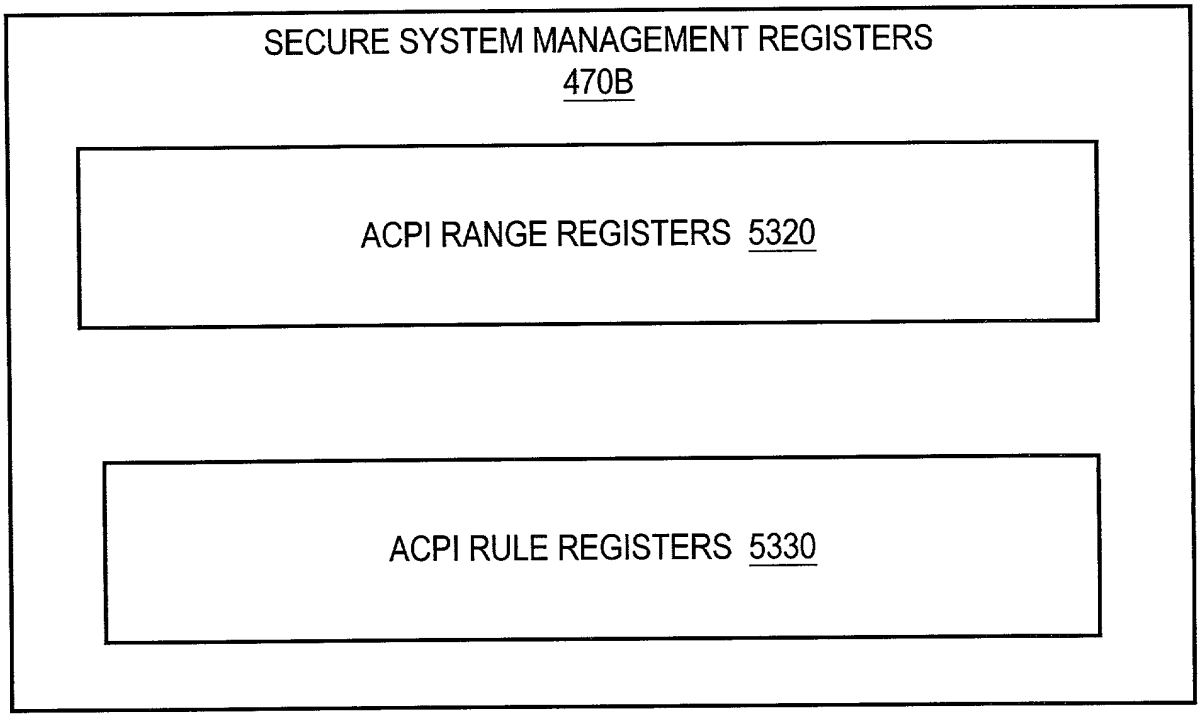


Fig. 42B